



CONSUMER ELECTRONICS AND THE IOT: DIGITAL EVIDENCE

LARS DANIEL, ENCE, CCLO, CCPA, CIPTS, CTNS, CTA, CWA
PRACTICE LEADER – DIGITAL FORENSICS AT ENVISTA FORENSICS

Chinese Social Credit System

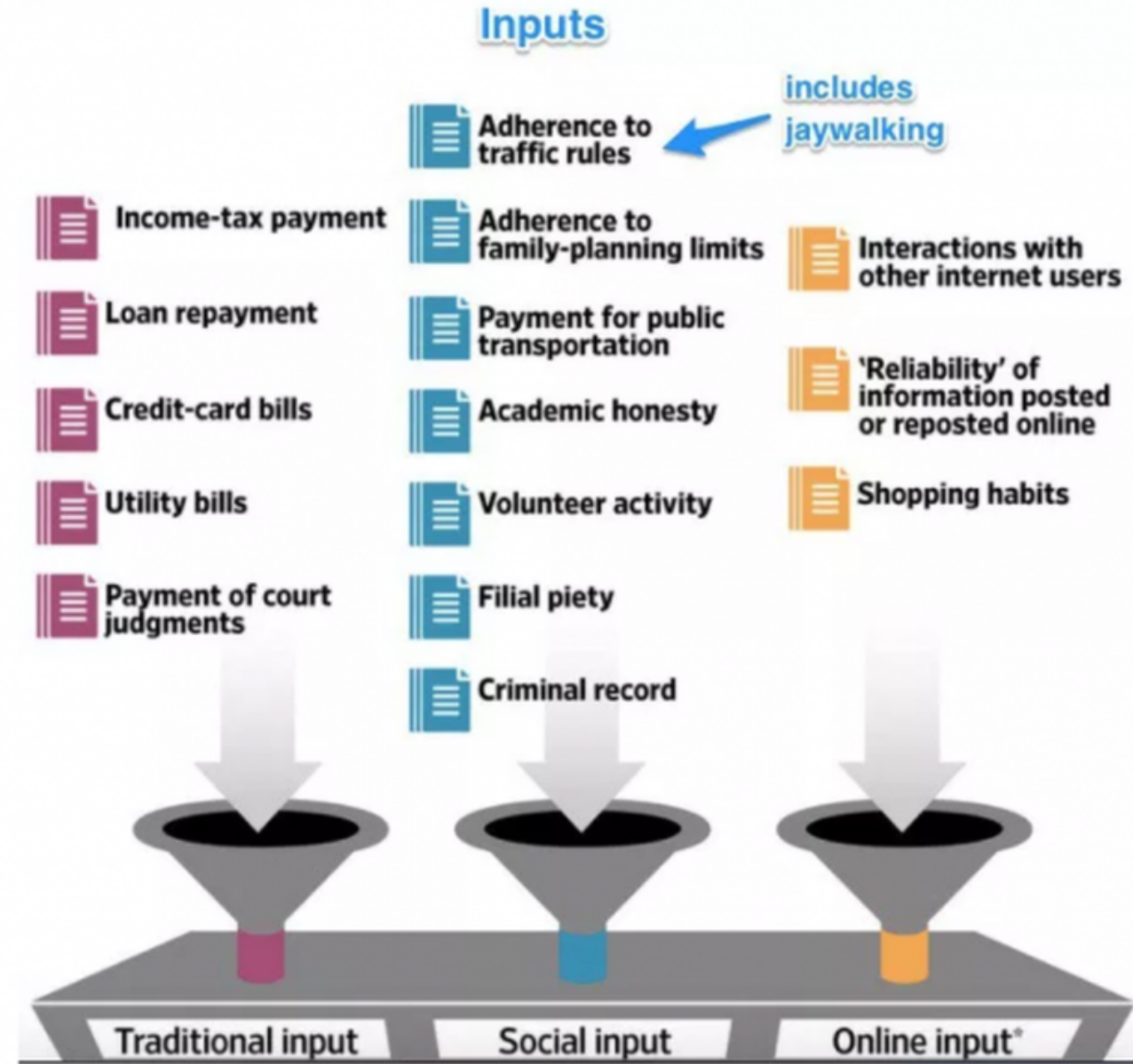


<https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking>

Chinese Social Credit System

- Inputs

- Traditional
- Social
- Online

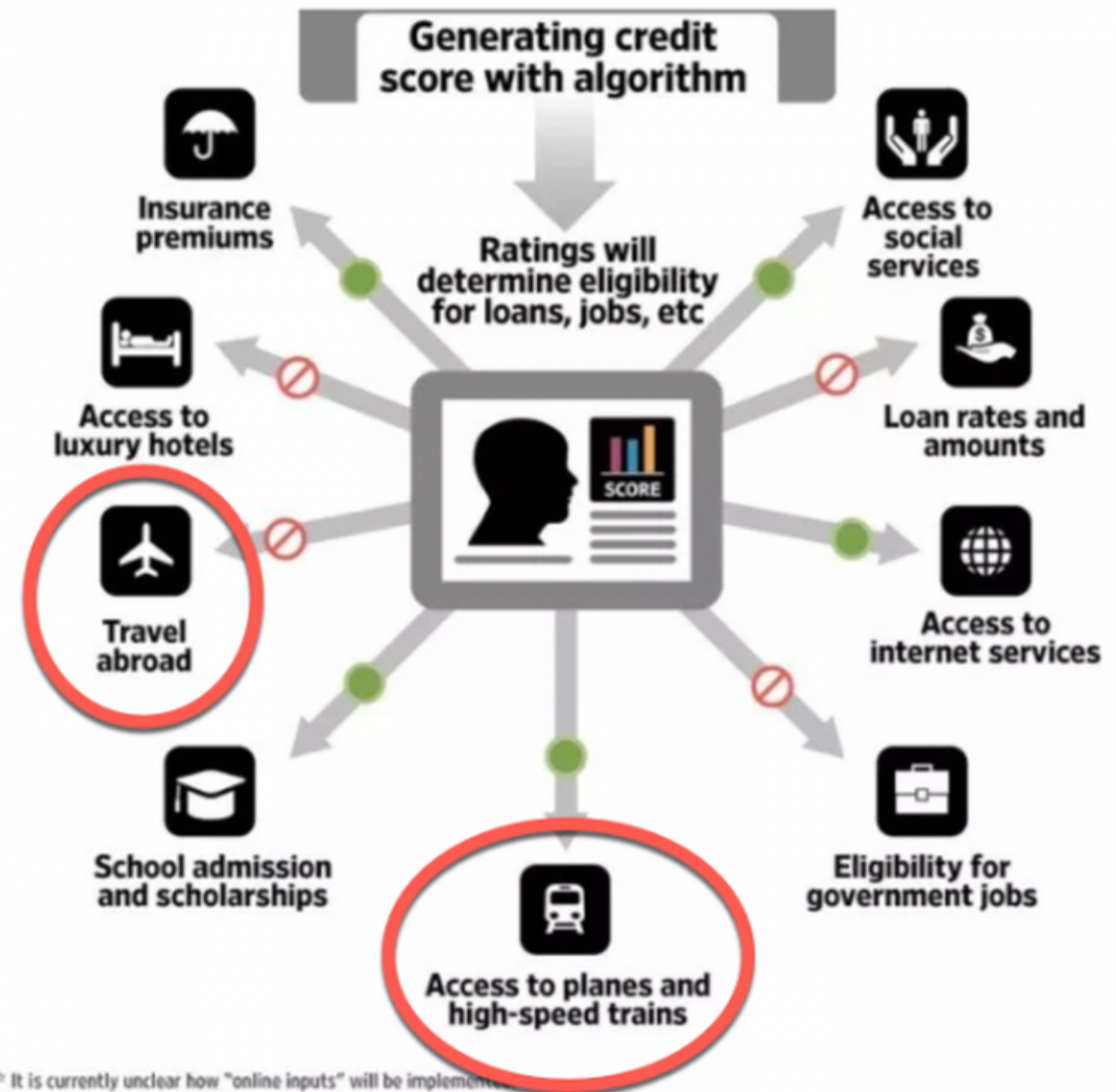


<https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking>

Chinese Social Credit System

- Banning you from flying or getting the train
- Throttling your internet speeds
- Banning you, or your kids, from the best school
- Stopping you getting the best jobs
- Keeping you out of the best hotels
- Getting your dog taken away
- Being publicly named as a bad citizen
- Unable to secure loans, credit cards, financial assistance

<https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking>



* It is currently unclear how "online inputs" will be implemented.
Source: WSJ reporting based on government blueprints, state-media reports and interviews with architects of the plan.

Chinese Social Credit System

- Facial Recognition
- 600+ AI Powered CCTV Cameras used for surveillance of citizens.



<https://medium.com/@ivonne.teoh/chinas-tech-companies-help-government-to-set-up-social-credit-system-by-2020-ebbd96bc0b06>

Chinese Social Credit System

- Facial Recognition

- Every movement of pupils at Hangzhou Number 11 High School in eastern China is watched by three cameras positioned above the blackboard. The "smart classroom behaviour management system," or "smart eye", is the latest highly-intrusive surveillance equipment to be rolled out in China, where leaders have rushed to use the latest technology to monitor the wider population... The computer will pick up seven different emotions, including neutral, happy, sad, disappointed, angry, scared and surprised.



<https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/>

Chinese Social Credit System

- Facial Recognition

- “Officers wear augmented-reality smartglasses that recognize facial features and license plates in near real time checking them against a database of subjects”



<https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/>

Lower Manhattan

- Facial Recognition

The **Domain Awareness System** is a surveillance system developed as part of [Lower Manhattan Security Initiative](#) in a partnership between the [New York Police Department](#) and [Microsoft](#) to monitor [New York City](#). This allows them to track surveillance targets and gain detailed information about them. The system is connected to 6,000 video cameras around New York City.



<https://www.cityandstateny.com/articles/opinion/commentary/new-york-should-regulate-law-enforcement-use-of-facial-recognition>

https://en.wikipedia.org/wiki/Domain_Awareness_System

Chinese Social Credit System

- Surveillance Drones

- Over recent years, more than 30 Chinese military and government agencies have reportedly been using drones made to look like birds to surveil citizens in at least five provinces, according to the South China Morning Post. The program is reportedly codenamed "Dove" and run by Song Bifeng, a professor at Northwestern Polytechnical University in Xi'an. Song was formerly a senior scientist on the Chengdu J-20, Asia's first fifth-generation stealth fighter jet, according to the Post. The bird-like drones mimic the flapping wings of a real bird using a pair of crank-rockers driven by an electric motor. Each drone has a high-definition camera, GPS antenna, flight control system and a data link with satellite communication capability, the Post reports.



<https://www.cnet.com/news/china-launches-high-tech-bird-drones-to-watch-over-its-citizens/?fbclid=IwAR3LwxkR81A99QKa72t4Cx1gGq3QBIShvEA0bPGmc0muCn9f4myPNGpHHHE>

Chinese Social Credit System

- Data Collection

- The Chinese government aims at assessing the trustworthiness and compliance of each person. Data stems both from peoples' own accounts, as well as their network's activities. Website operators can mine the traces of data that users exchange with websites and derive a full social profile, including location, friends, health records, insurance, private messages, financial position, gaming duration, smart home statistics, preferred newspapers, shopping history, and dating behavior.

- Algorithms

- Automated algorithms are used to structure the collected data, based on government rules

Data Collection in the USA

- Data Collection

- License Plate Databases
 - License plate records and geo-tagged photos
- Credit Reporting Agencies
 - Collect sensitive data and sell it to banks, creditors, insurers...
- Smartphone Location Tracking
 - Extremely precise, allows for real time traffic, location busyness...
 - Google tells you how busy the gym or restaurant is at a particular time
- Digital Ads/Purchases
 - Location data sold to retailers (online and brick and mortar) to generate targeted ads.
- Smart Home Objects
 - iRobot Roomba mapping your home

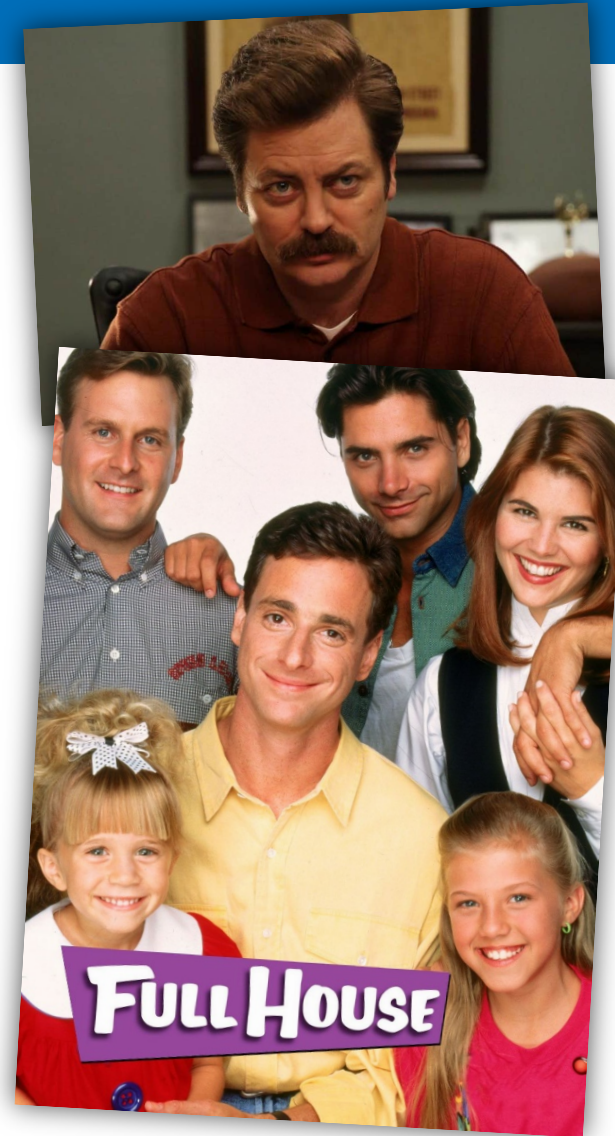
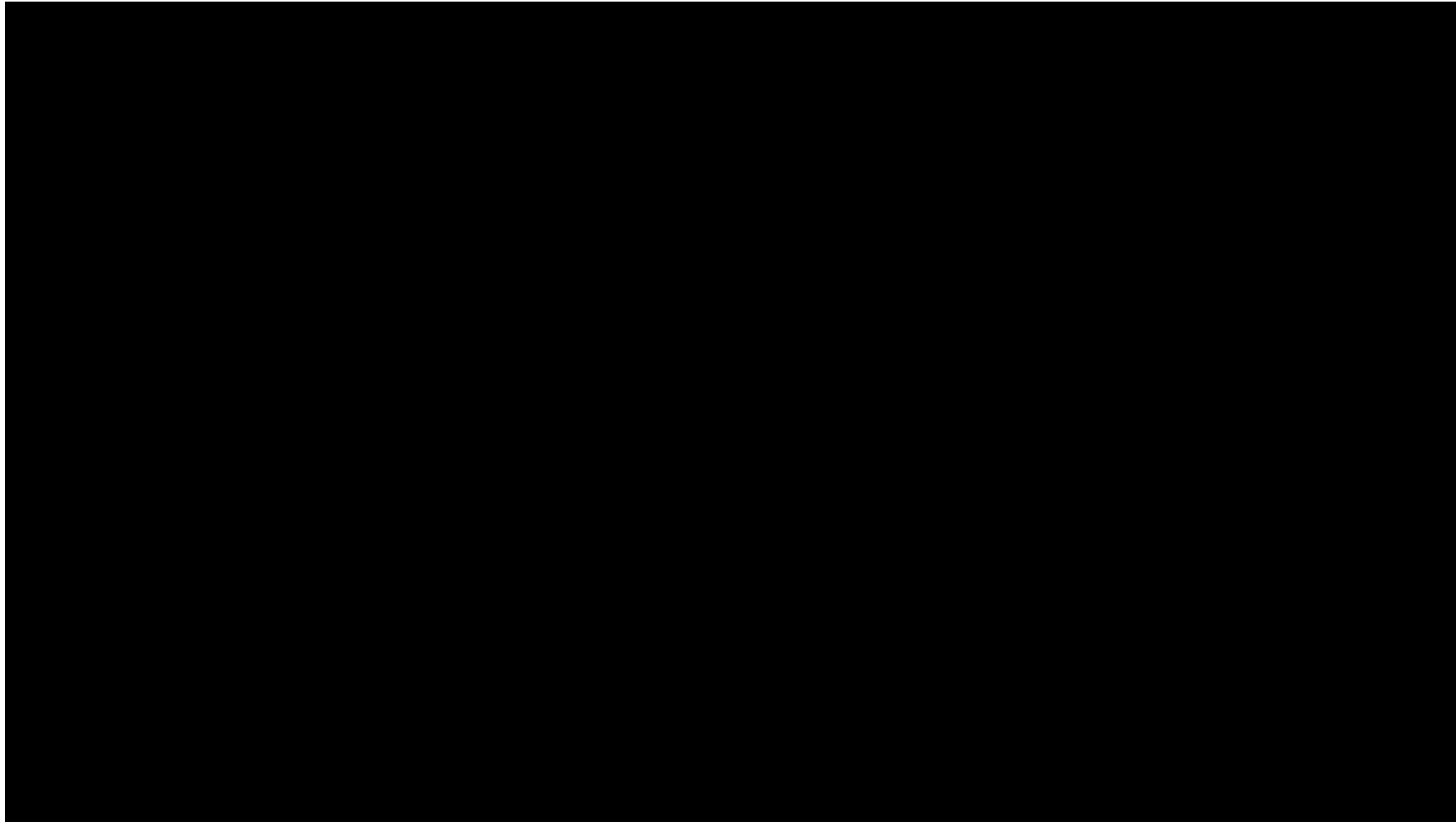
Chinese Social Credit System

- For example, buying something like diapers is seen as “responsible” and will improve your score, while things like video games are seen as idle and irresponsible and will bring your score down.
- your score also goes up or down based on interaction with friends who have a higher or lower score than you. Meaning, if a friend is given a low score and therefore deemed “less trustworthy,” you would be urged to spend less time with that person...(by Gov’t)



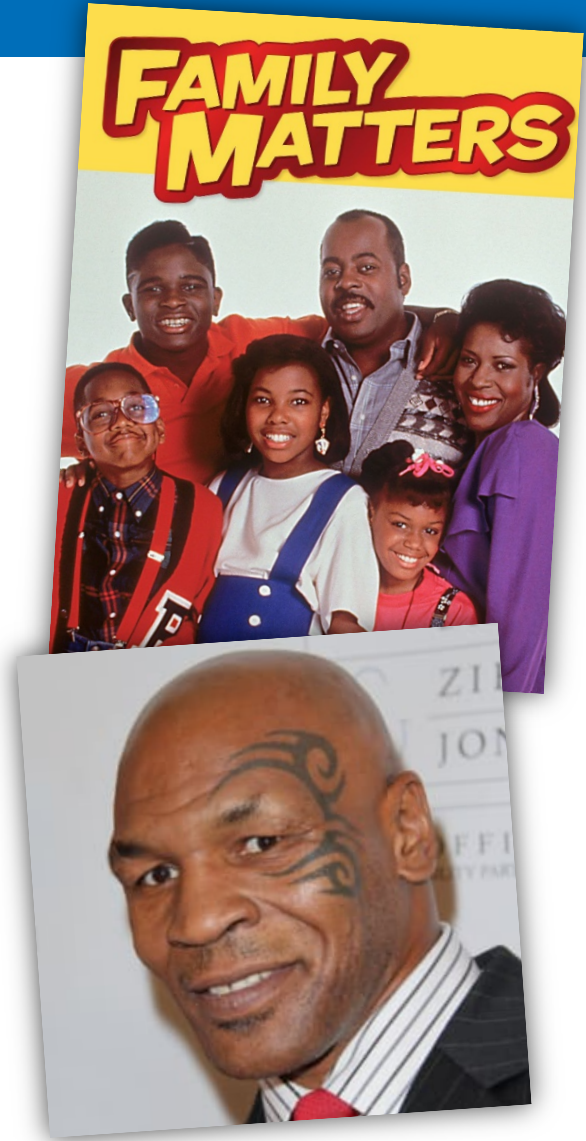
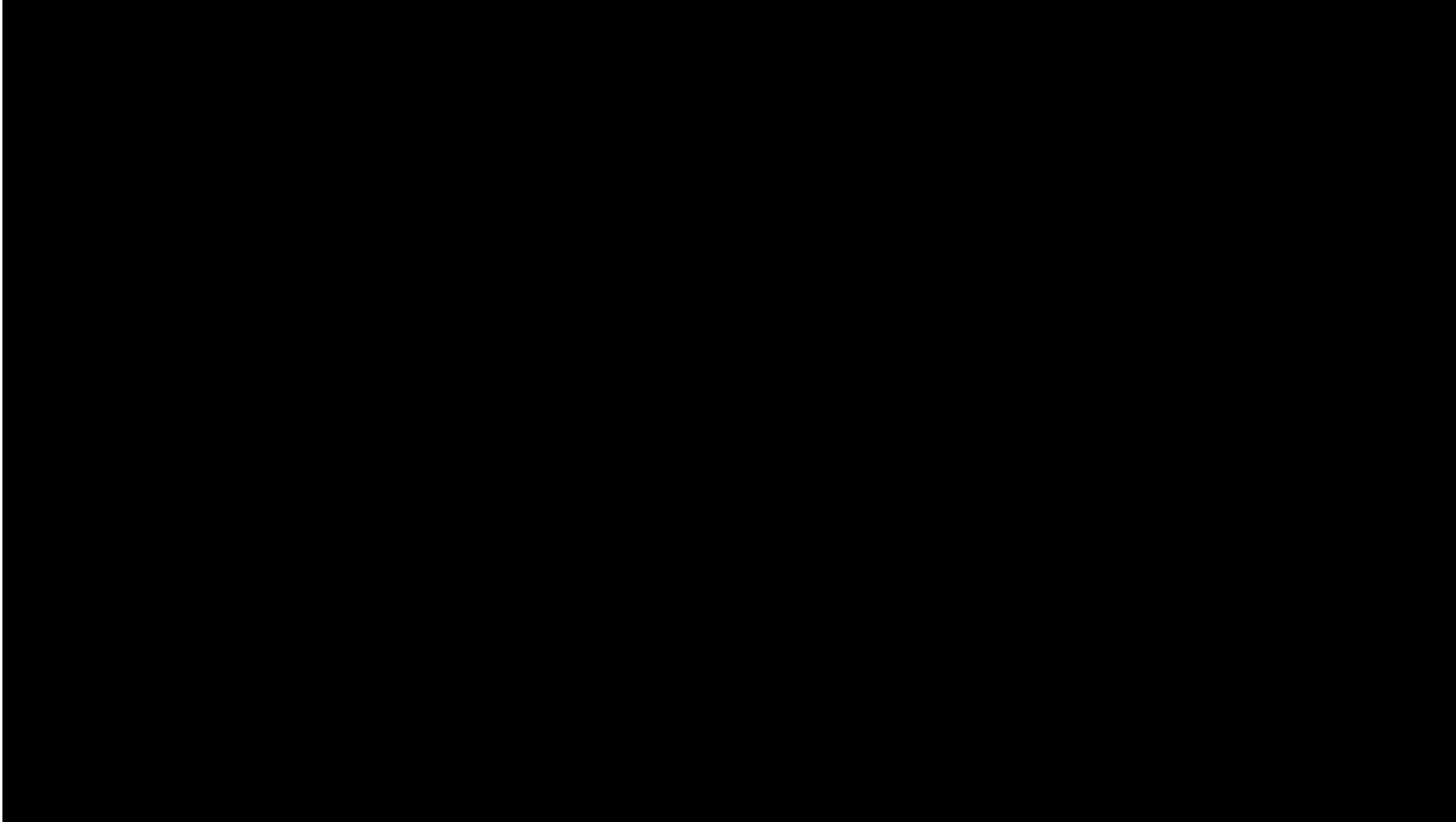
What determines the “truth” of content?

- Deepfake Videos — Nick Offerman



Will sharing this lower your score?

- Deepfake Videos — Mike Tyson



The Fake News Problem – what about this?





WHAT IS THE IOT?

Internet of Things (IoT)

- What is the Internet of Things?

- 1980's

- Carnegie Mellon University

- Programmers would connect via the internet to the Coke machine to see if a drink was available, and if it was cold.



```
> In the mid-seventies expansion of the department caused people's
> offices to be located ever further away from the main terminal room
> where the Coke machine stood. It got rather annoying to traipse down
> to the third floor only to find the machine empty - or worse, to shell
> out hard-earned cash to receive a recently loaded, still-warm Coke.
> One day a couple of people got together to devise a solution.
>
> They installed micro-switches in the Coke machine to sense how many
> bottles were present in each of its six columns of bottles. The
> switches were hooked up to CMUA, the PDP-10 that was then the main
> departmental computer. A server program was written to keep tabs on
> the Coke machine's state, including how long each bottle had been in
> the machine. When you ran the companion status inquiry program, you'd
> get a display that might look like this:
>
>                EMPTY    EMPTY    1h 3m
>                COLD     COLD     1h 4m
>
> This let you know that cold Coke could be had by pressing the
> lower-left or lower-center button, while the bottom bottles in the two
> right-hand columns had been loaded an hour or so beforehand, so were
> still warm. (I think the display changed to just "COLD" after the
> bottle had been there 3 hours.)
```

Internet of Things (IoT)

- What is the Internet of Things?
 - Any device with that is connected to the internet
 - Shared processing power
 - The **Internet of Things (IoT)** is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data



Petchatz.com

Internet of Things (IoT)

- Milestones

- Barcode Reader

- 1952

- First ever built in a New York apartment by Norman Joseph and Bernard Silver
 - Ability to create and store data for retailers, shipping, inventory management...powerful when coupled with RFID



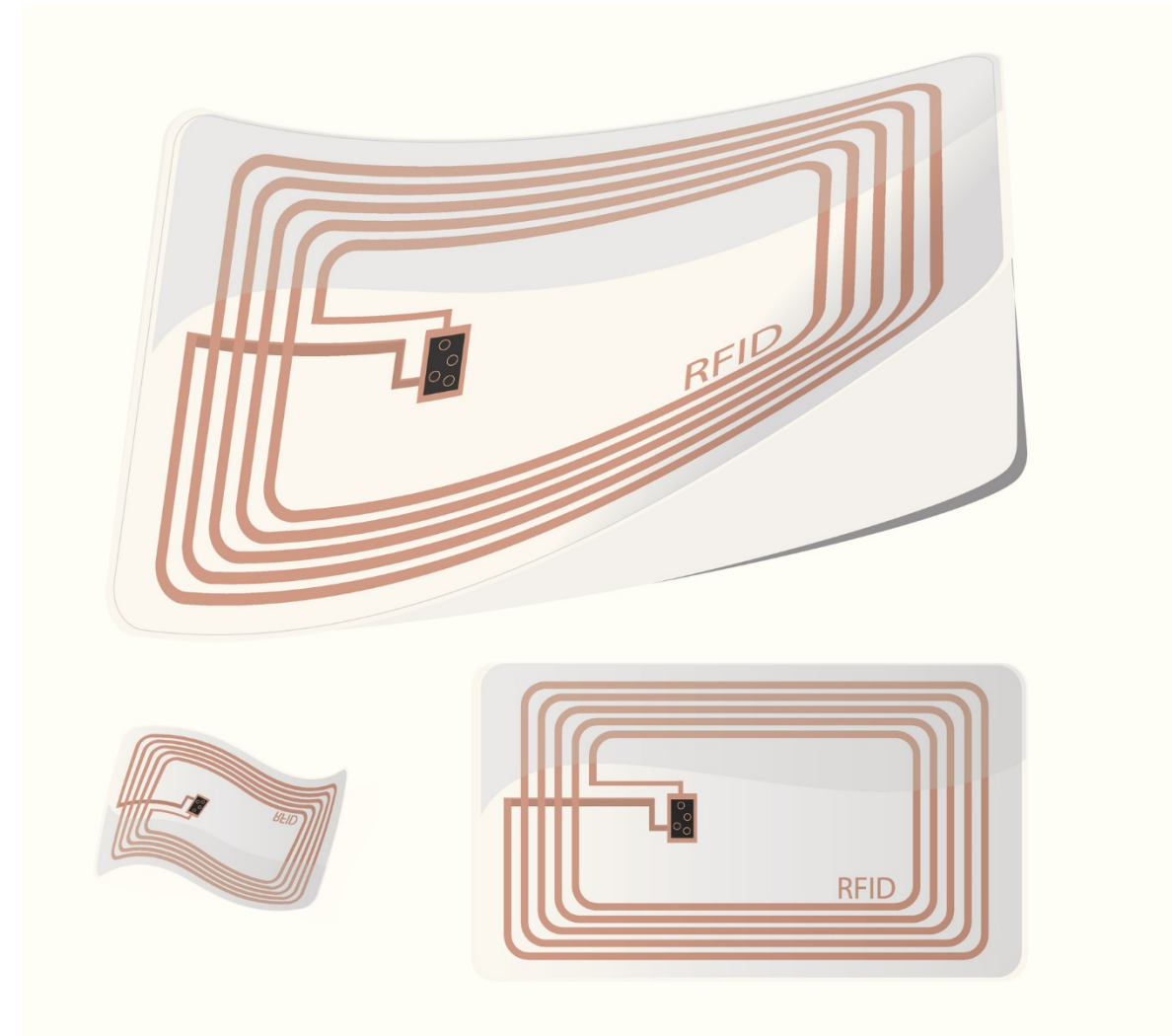
Internet of Things (IoT)

- Milestones

- RFID

- 1990's (becomes commonplace)

- Automatic tracking without the need for a human to scan or capture data
 - Much more efficient than barcodes



Internet of Things (IoT)

- Milestones

- Sensors

- Everything talks to everything
 - Stores and transmits data
 - Talks to RFID



Internet of Things (IoT)

- Milestones

- Big Data / Cloud
 - 2008-2009
 - According to [Cisco Internet Business Solutions Group](#) (IBSG), the Internet of Things was born in between 2008 and 2009 at simply the point in time when more “things or objects” were connected to the Internet than people.
 - 12.5 billion connected devices in 2010
- Why is needed
 - Ability to store and transmit massive amounts of data generated by devices, sensors, websites, applications, etc.

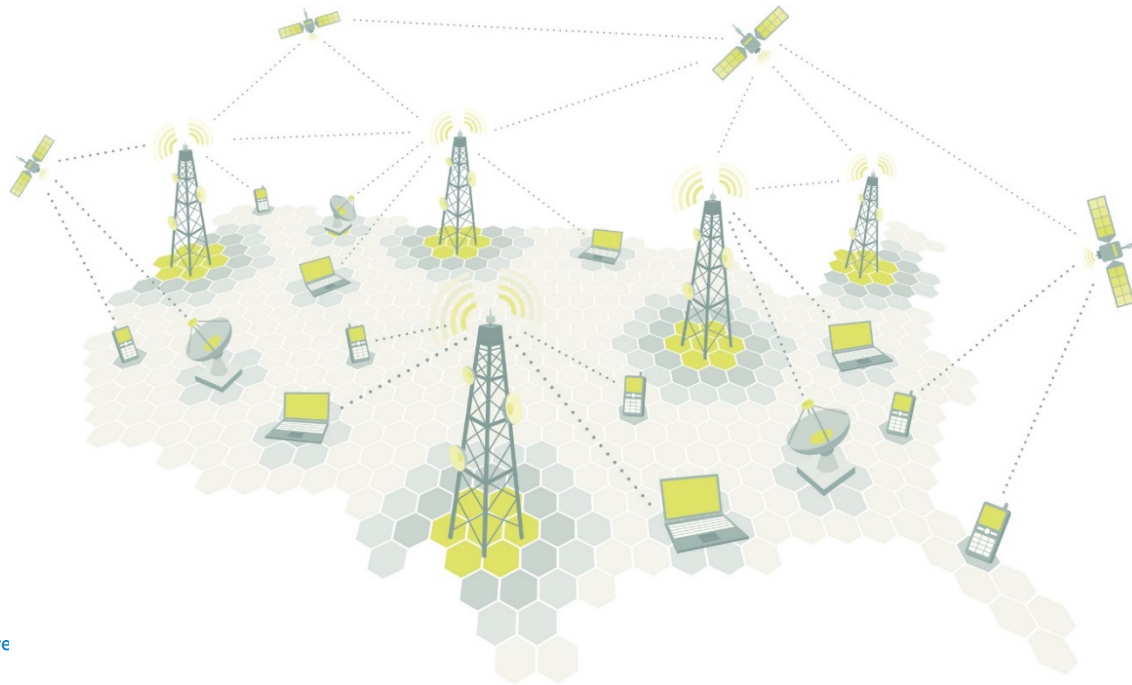


Internet of Things (IoT)

- Cellular Network

- Big Data / Cloud

- Around 29 billion connected devices¹ are forecast by 2022, of which around 18 billion will be related to IoT
 - 90% of the world covered by cellular signal
 - 70% of wide-area IoT devices will use cellular technology in 2022
 - LTE and Beyond





IOT DEVICES

IoT Devices

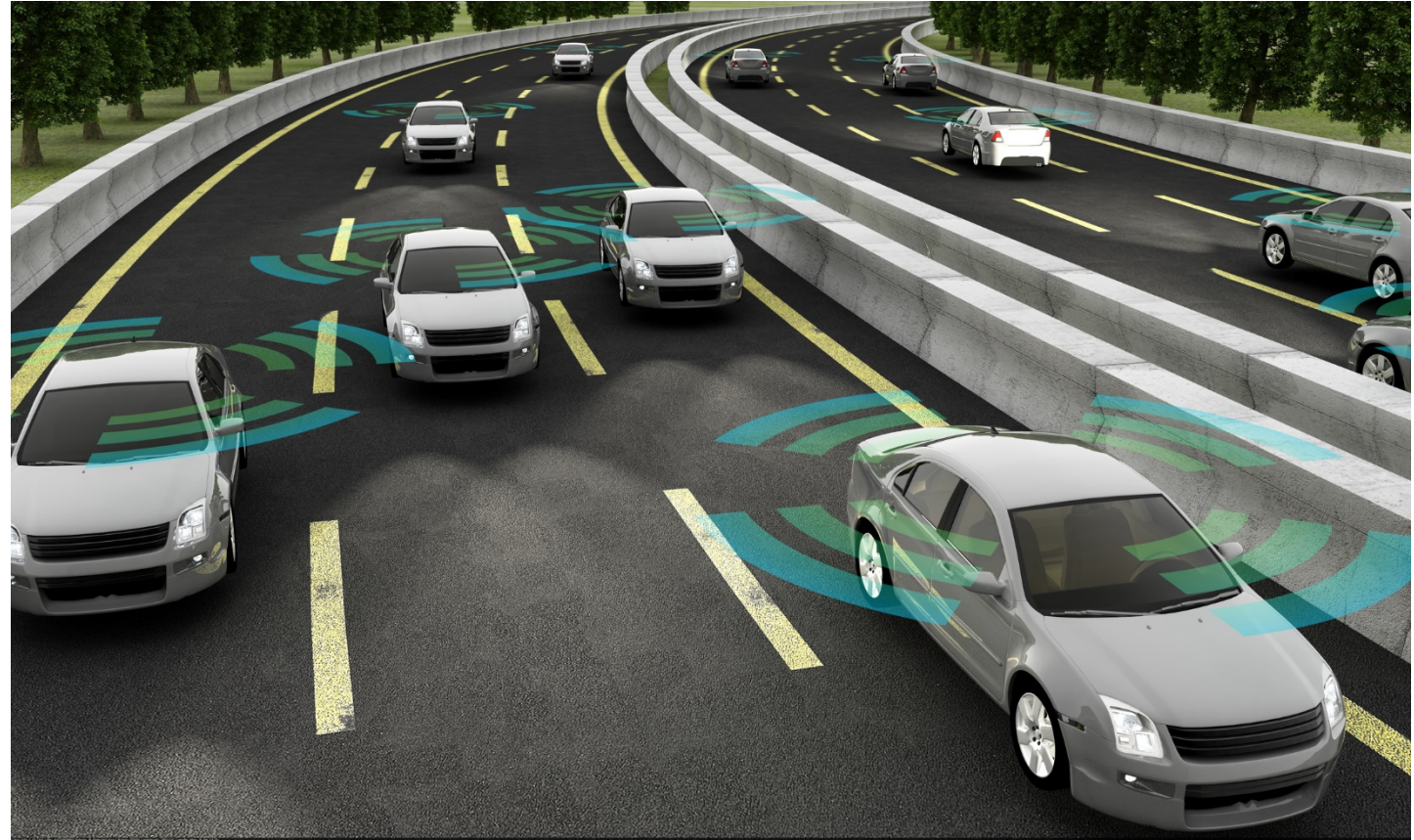
- Always on devices
 - Always listening...?
 - Data collection
 - Data stored on local devices
 - Cell phones, computers
 - Data stored in the cloud
 - Association accounts



IoT Devices

- Vehicles

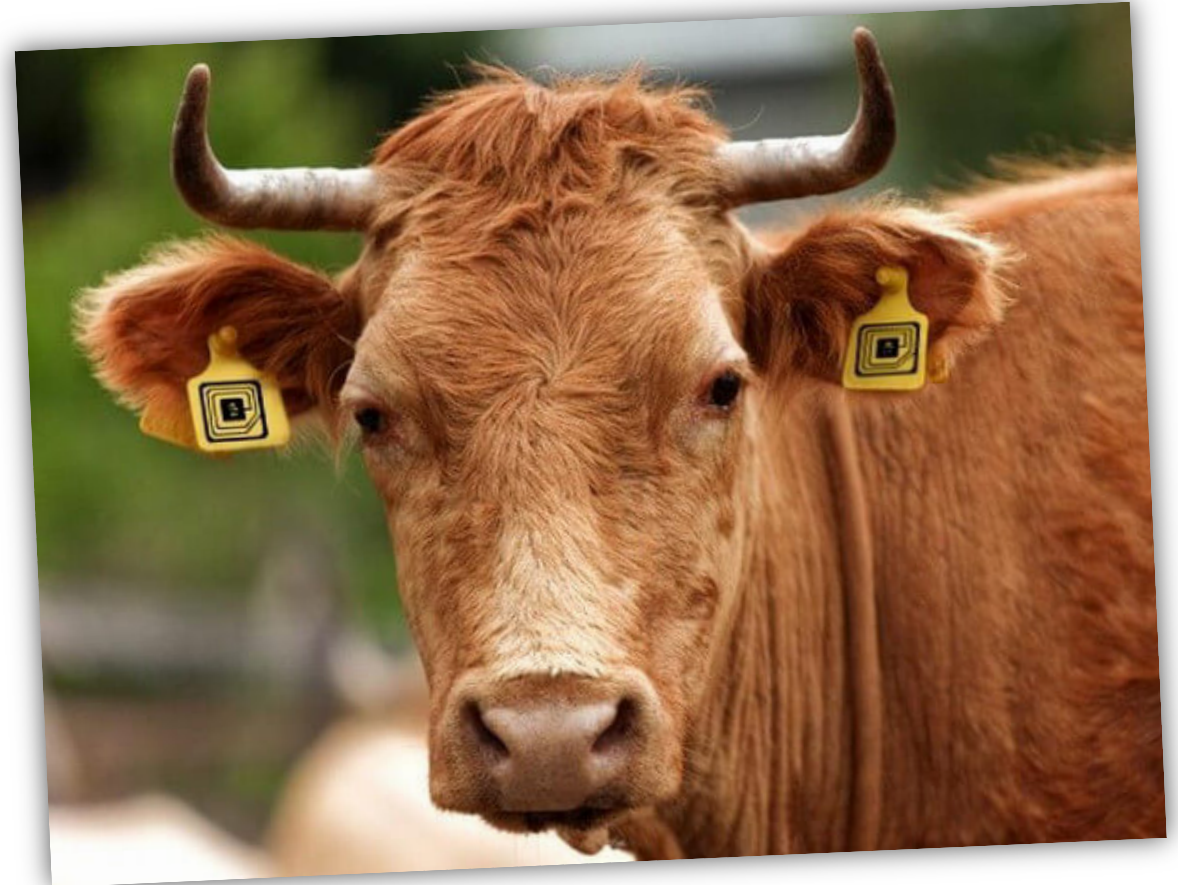
- Cellular connection
- Autonomous
- Semi-autonomous
- Video
 - Tesla “Summon”



IoT Devices

- Wearable technology

- Beyond fitness!
- Medical
 - Athletic performance, medical analytics
- Logistics
 - People movement, animal movement
 - Livestock are one of the first uses of IoT, including tracking movement, fertility, behavior, lactation...
- Government
 - Tracking, monitoring



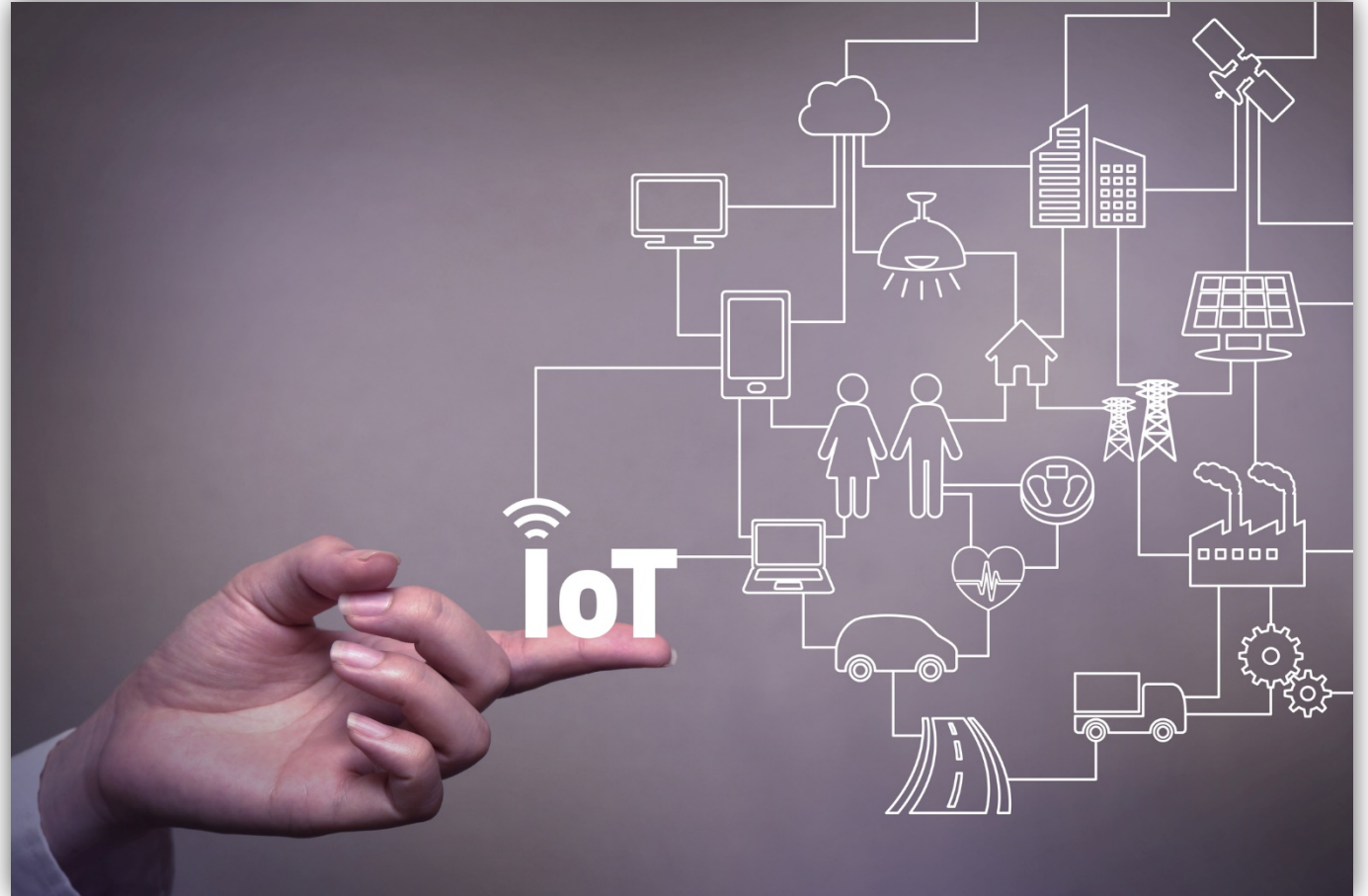
Digital Forensics - Murder Cases

- Case Example
 - SODDI Defense
 - (Some Other Dude Did It)
 - Computer Forensics
 - Cell Phone Forensics
 - Cellular Location
 - Xbox Forensics
 - Alarm System Logs



Internet of Things (IoT)

- What the Future Holds
 - Hyper-connection is the future, and it is coming fast.





IOT CYBER SECURITY

TODAY'S HACKING = TOMORROW'S EVIDENCE

IoT Security Risks

- Hacking

- millions of insecure connected devices
- Leaves critical systems and data around the world at risk



IoT Hacking Tools and Techniques

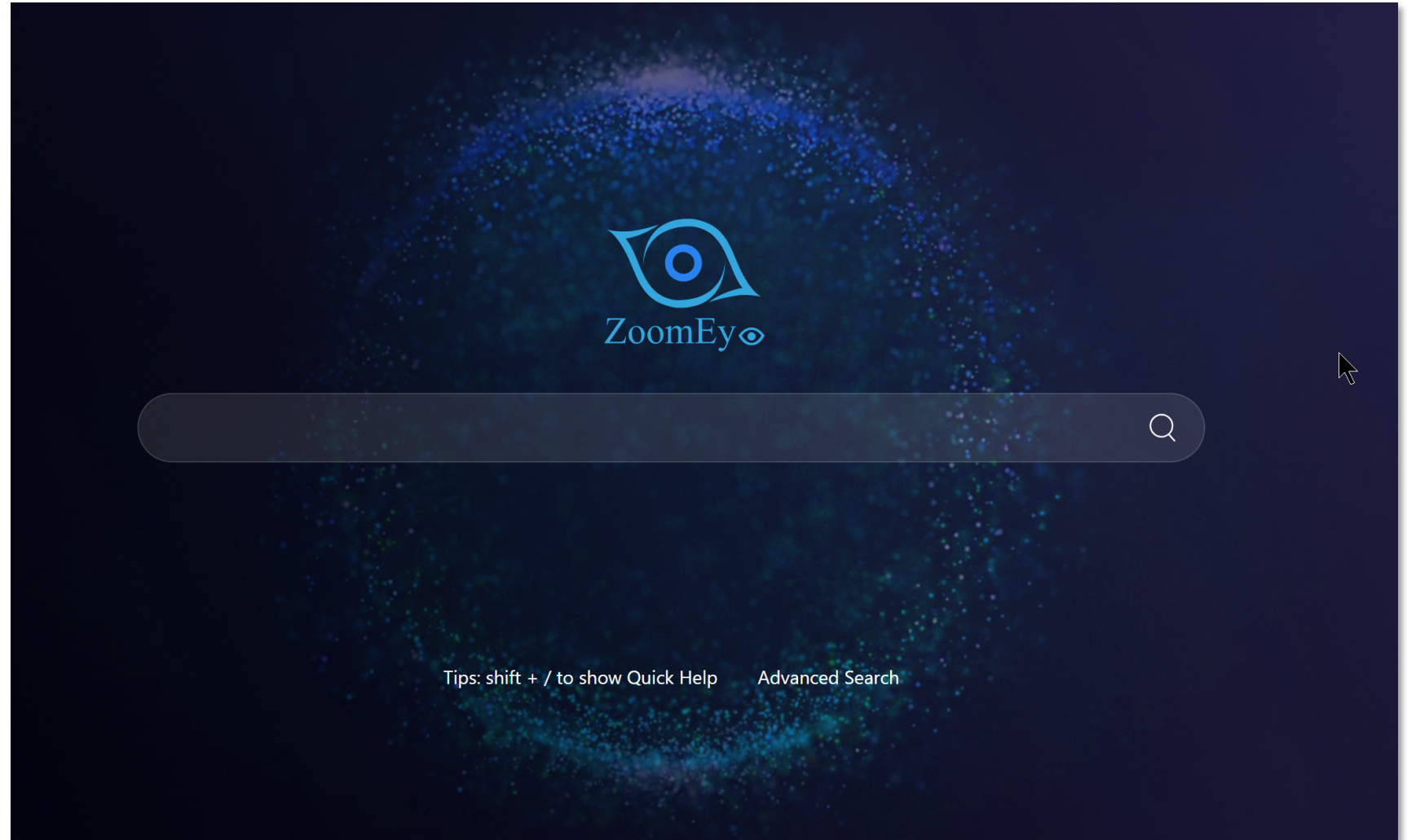
- Finding Attackable Hosts –

- There are three difference search engines that scan for open ports and vulnerable services:

- Censys.io
- Zoomeye.org
- Shodan.io

IoT Hacking Tools and Techniques

- Zoomeye.org



IoT Hacking Tools and Techniques

ZoomEy

[Home](#)[Explore](#)[Developer](#)[Lab](#)[Enterprise](#)

...

+port:"8080" +service:"http"

Search

User

Menu

World Map

-

+

Year

2018	8,330,176
2017	6,771,864
2016	2,823,164
2015	3,113,322
2014	616,499

Country

United States	6,267,238
Mexico	1,767,500
Brazil	1,246,287
Republic of Korea	964,268

Result

Vulnerability

About 21,655,025 results 0.367 seconds

+port:"8080" X

+service:"http" X

38.117.101.212

8080/http

Canada, Toronto

2018-05-31 21:16

38.117.74.3

8080/http

United States, Beverly Hills

2018-05-31 21:16

HTTP/1.1 403 Forbidden

Content-Type: text/html; charset=utf-8

Content-Length: 106

Connection: close

HTTP/1.1 302 Found

Cache-Control: private

Expires: Wed, 31 Dec 1969 19:00:00 EST

Location: https://localhost/

Content-Length: 0

Date: Thu, 31 May 2018 13:16:31 GMT

Contribute

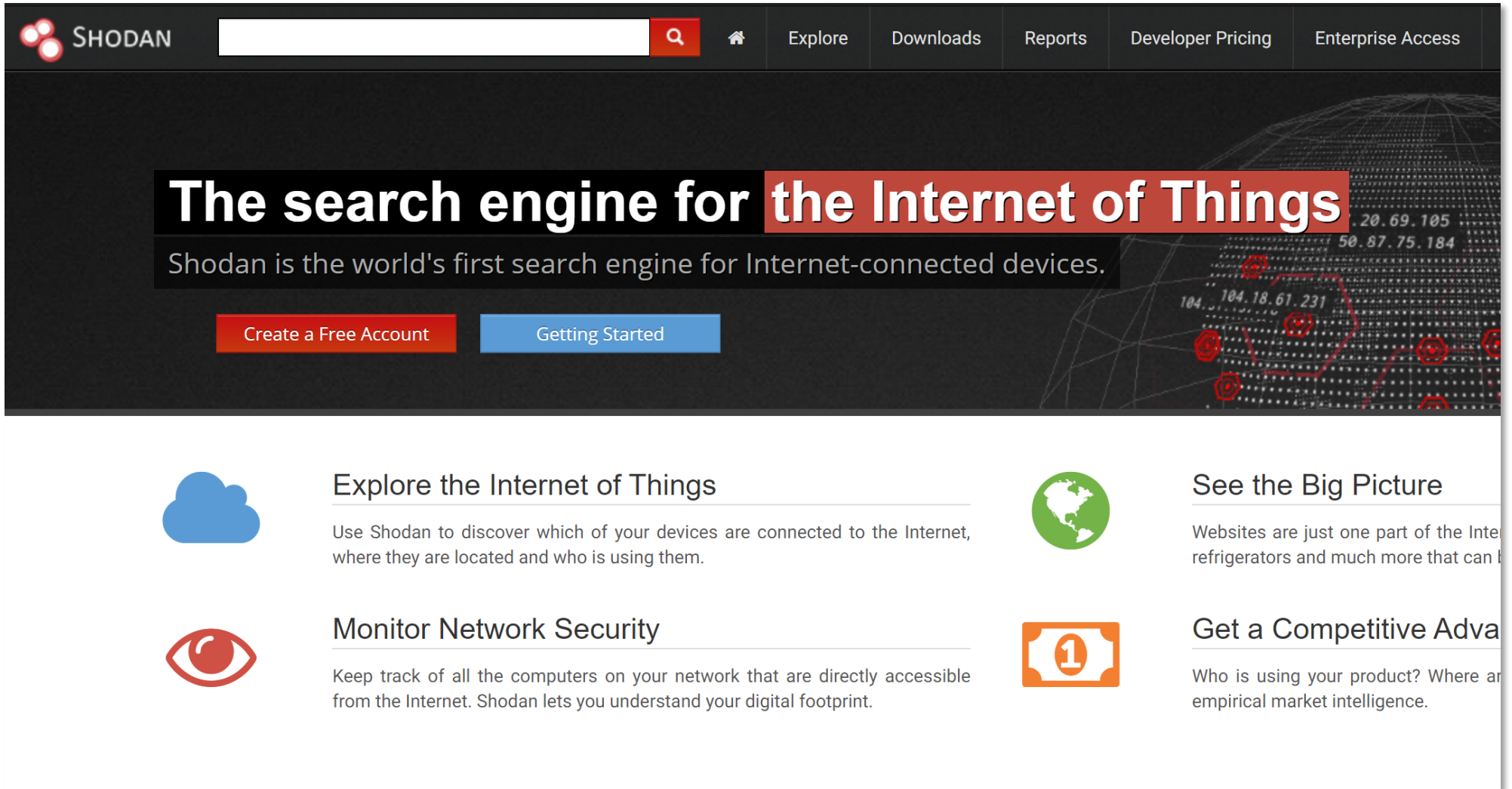
Dork

34 of 89

© 2020 Envista Forensics

IoT Hacking Tools and Techniques

- Shodan.io



The screenshot shows the Shodan.io homepage. At the top is a navigation bar with the Shodan logo, a search bar, and links for Explore, Downloads, Reports, Developer Pricing, and Enterprise Access. The main banner features the headline "The search engine for the Internet of Things" with "the Internet of Things" highlighted in a red box. Below this is the subtext "Shodan is the world's first search engine for Internet-connected devices." and two buttons: "Create a Free Account" and "Getting Started". The background of the banner shows a network map with IP addresses like 20.69.105 and 50.87.75.184. Below the banner are four feature sections: "Explore the Internet of Things" (with a cloud icon), "Monitor Network Security" (with an eye icon), "See the Big Picture" (with a globe icon), and "Get a Competitive Advantage" (with a number 1 icon). Each section has a brief description of its functionality.

SHODAN

Explore Downloads Reports Developer Pricing Enterprise Access

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

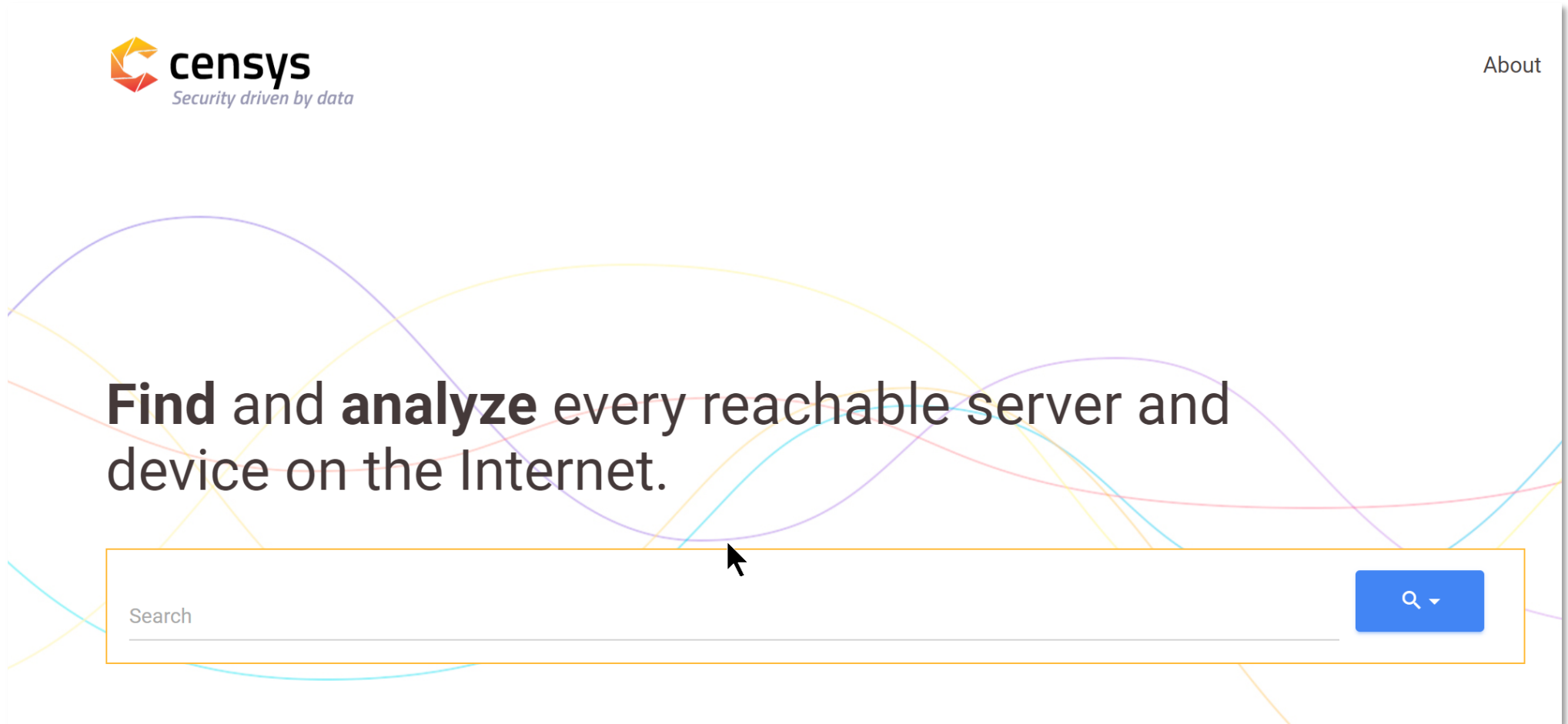
Websites are just one part of the Internet. Shodan lets you see the big picture, including refrigerators and much more that can be connected to the Internet.

Get a Competitive Advantage


Who is using your product? Where are they using it? Shodan provides empirical market intelligence.

IoT Hacking Tools and Techniques

- Censys.io



IoT Hacking Tools and Techniques



Q IPv4 Hosts

(webcam) AND protocols.raw: "8080/http"

NT

Tag:

6,029 http

1,376 https

1,307 ssh

838 ftp

524 smtp

More

[173.254.8.244 \(173-254-8-244.unifiedlayer.com\)](#)

Unified Layer (46606)

Provo, Utah, United States

110/pop3, 143/imap, 21/ftp, 443/https, 80/http, 8080/http, 993/imap, 995/pop3s

Webcam Modeling - Eye Candy Web Models - Live Webcam Jobs *.bluehost.com, bluehost.com

8080.http.get.title: Webcam Modeling - Eye Candy

[92.190.169.78](#)

AS (12479)

France

8080/http

8080.http.get.body: 1]
 Webcam

[23.92.77.79 \(as125.vacares.com\)](#)

Inzero LLC (54540)

United States

110/pop3, 143/imap, 21/ftp, 25/smtp, 443/https, 53/dns, 80/http, 8080/http, 993/imap, 995/pop3s

Cams Of The Web - Recorded Live Webcam Porn Feeds camsoftheweb.com, www.camsoftheweb.com

8080.http.get.title: Live Webcam Porn Feeds

[79.230.189.22 \(p4FE6BD16.dip0.t-ipconnect.de\)](#)

DTAG Internet service provider operations (3320)

Siegen, North Rhine-Westphalia, Germany

8080/http

8080.http.get.metadata.product: Webcam

[37.201.103.190 \(ip-37-201-103-190.hsi13.unitymediagroup.de\)](#)

UPC formerly known as UPC Broadband Holding B.V.... (6830)

Frankfurt am Main, Hesse, Germany

Entrolink DSL/cable Modem Win32 443/https, 8080/http

protocols: 8080/http

DSL/CABLE MODEM

EMBEDDED

IoT Hacking Tools and Techniques

- Live Webcam

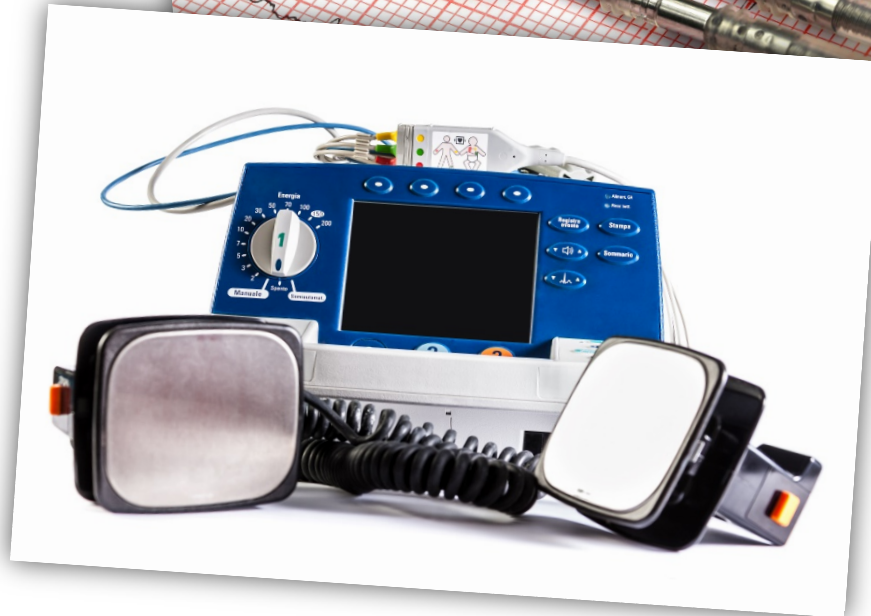
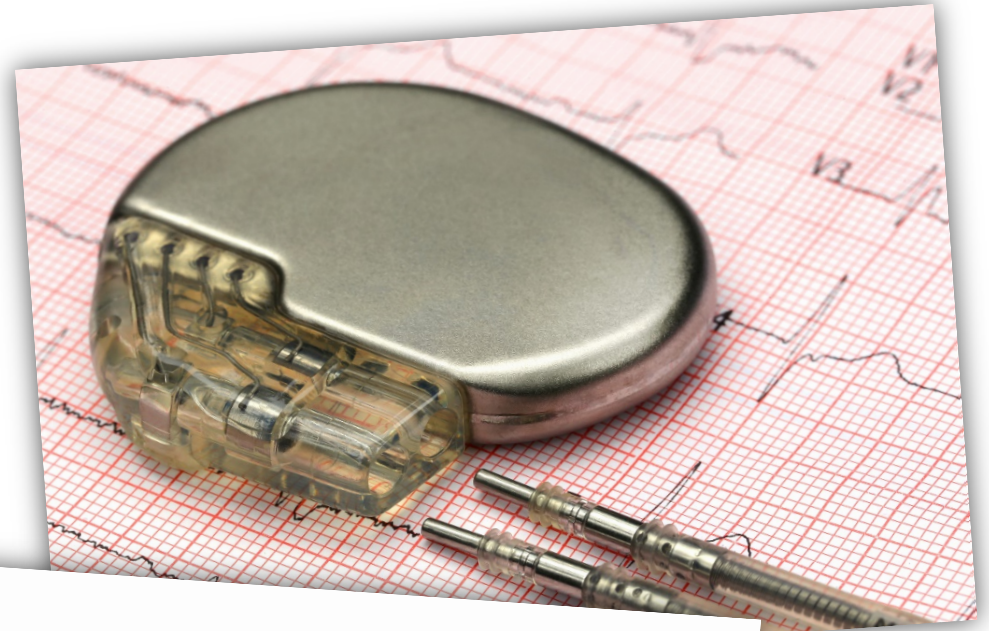


IoT Security Risks

- Hacking

- Cardiac devices

- Early this year, [CNN](#) wrote, “The FDA confirmed that St. Jude Medical’s implantable cardiac devices have **vulnerabilities that could allow a hacker to access a device**. Once in, they could deplete the battery or **administer incorrect pacing or shocks**, the FDA said.
 - “The vulnerability occurred in the transmitter that reads the device’s data and remotely shares it with physicians. **The FDA said hackers could control a device by accessing its transmitter.**”

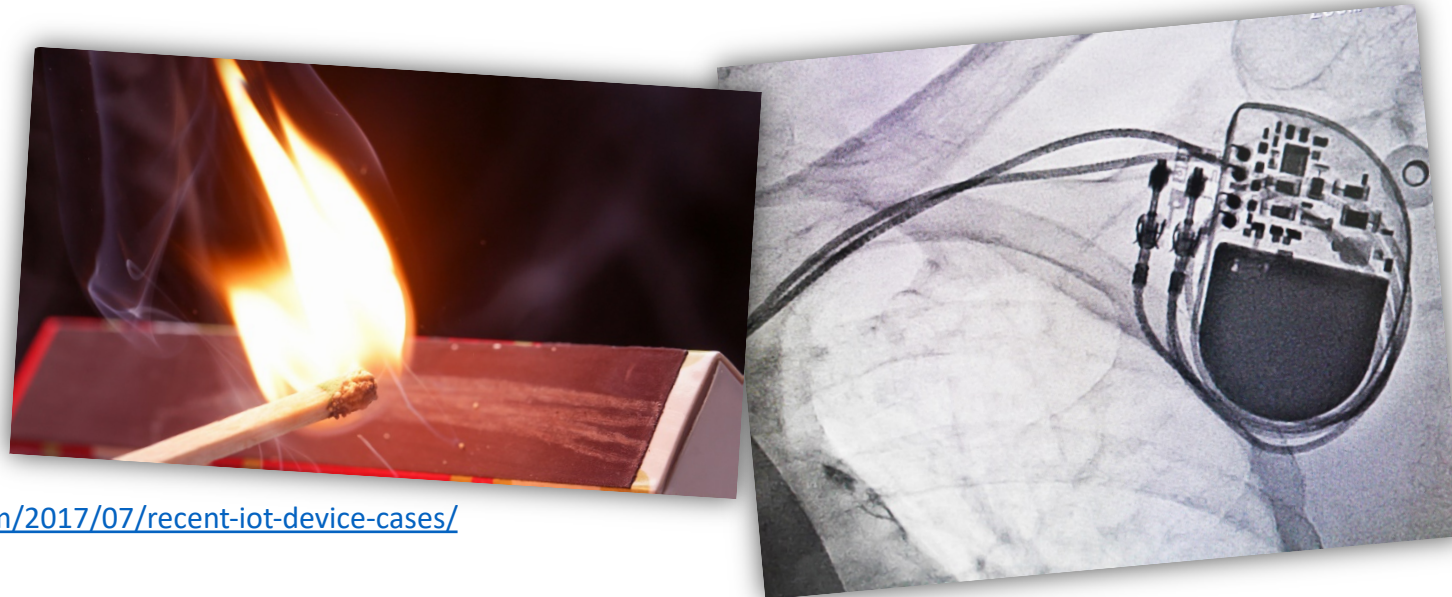


<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>

Who cares about Pacemaker data?

- Home arson case

- **pacemaker:** In a home arson case, the homeowner told police that he did a number of things as soon as he discovered the fire: he gathered his belongings, packed them in a suitcase and other bags, broke out the bedroom window with his cane, threw his belongings outside, and rushed out of the house. The police searched the 59-year old's pacemaker. Its data showed that the man's heart rate barely changed during the fire. And after a cardiologist testified that it was "highly improbable" that a man in his condition could do the things claimed, the man was charged with arson and insurance fraud.



<https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>

IoT Security Risks

- Hacking

- Owlet Baby Monitor

- Alerts parents if baby is having heart trouble
 - Hackers could cause false signals or cause device to stop reporting



<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>

IoT Security Risks

- Hacking

- TRENDnet Webcam Hack
 - TRENDnet transmitted user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers' login information in clear, readable text on their mobile devices, the FTC said.
 - Allowed hackers to watch the video feed from the camera in real time.



<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>

IoT Security Risks

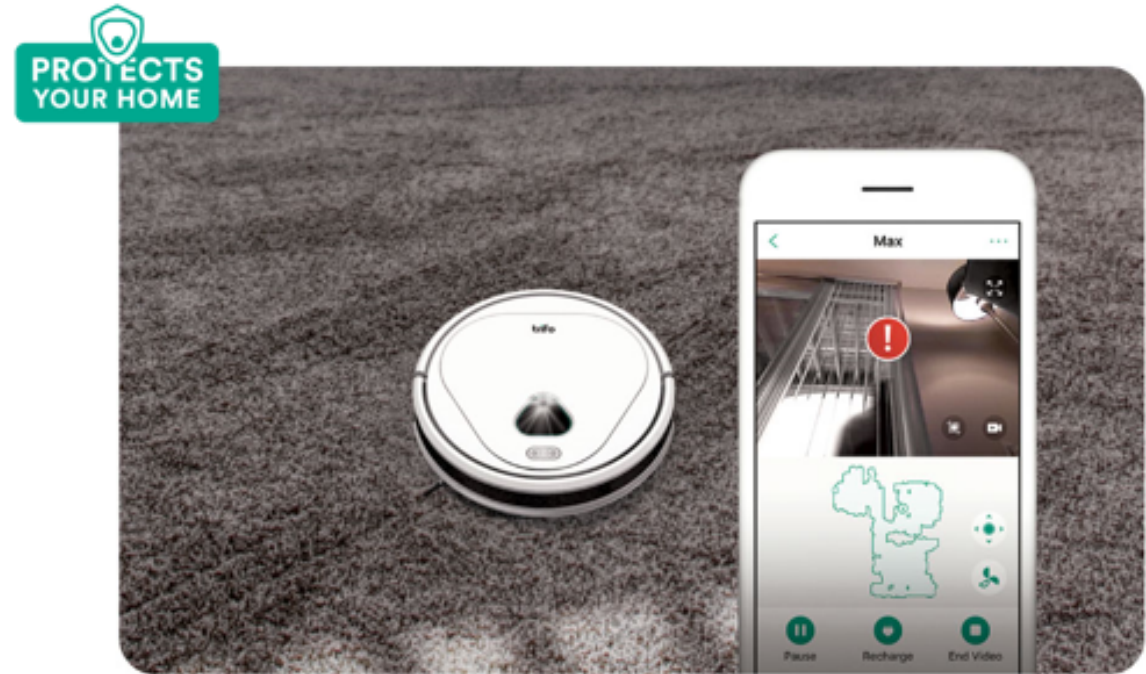
- Hacking

- Robot Vacuum Cleaner

- According to researchers with Checkmarx, the vacuum has several high-severity flaws that open the device to remote attacks. Those include a denial of service (DoS) attack that bricks the vacuum, to a hack that allows adversaries to peer into private homes via the vacuum's embedded camera.

I'm Protective

I care about our home. When you're not around, my motion and audio detection system knows when something is not right. Set up alert notifications, trigger automatic video recording and schedule patrolling times right from the Trifo Home App.



<https://threatpost.com/vacuum-cleaners-baby-monitors-and-other-vulnerable-iot-devices/153294/>

IoT Security Risks

- Hacking

- Industrial Robot Arm

- At the IEEE Security & Privacy conference later this month, they plan to present a case study of attack techniques they developed to subtly sabotage and even fully hijack a 220-pound industrial robotic arm capable of welding gripping claws, welding tools, or even lasers.



<https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/>

IoT Security Risks

- Physical Ransomware..?
- DDOS Attacks
 - Hackers are actively searching the internet and hijacking smart door/building access control systems, which they are using to launch DDoS attacks, according to firewall company SonicWall...(due to the type of exploit) meaning it can be exploited remote, even by low-skilled attackers without any advanced technical knowledge...these vulnerable systems can also be used as entry points into an organization's internal networks.

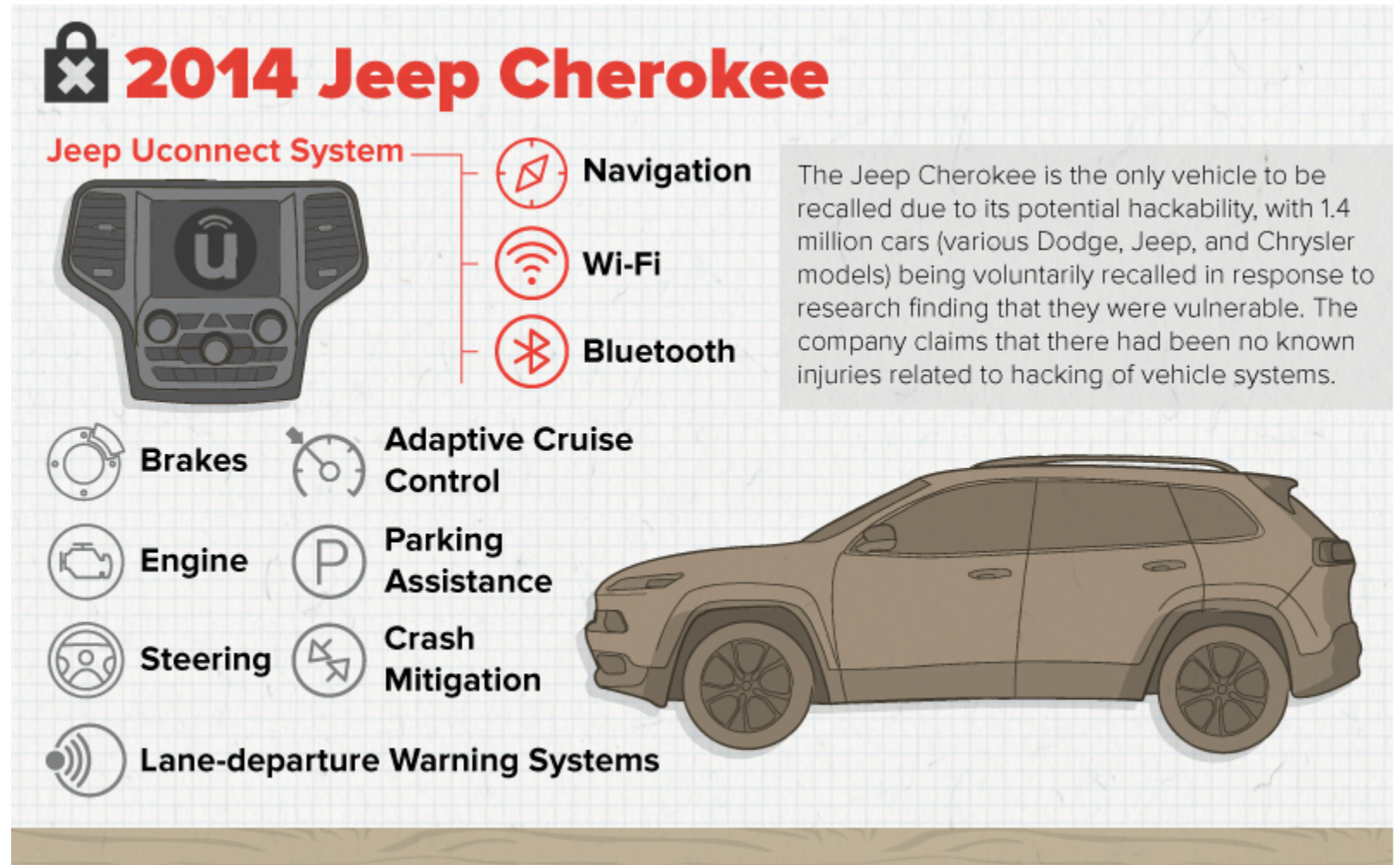


<https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/>

IoT Security Risks

- Hacking

- Connected vehicles

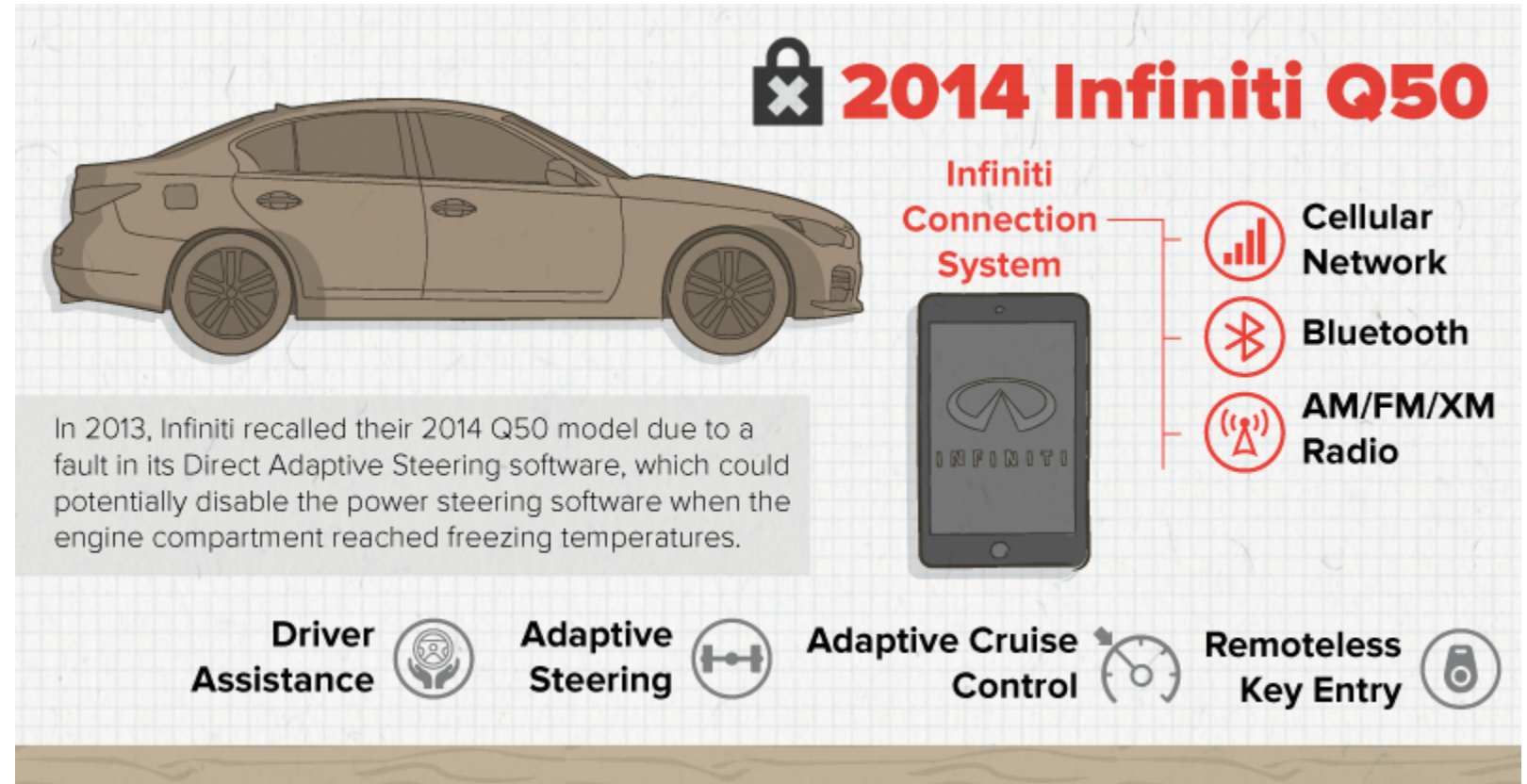


<https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1>

IoT Security Risks

- Hacking

- Connected vehicles

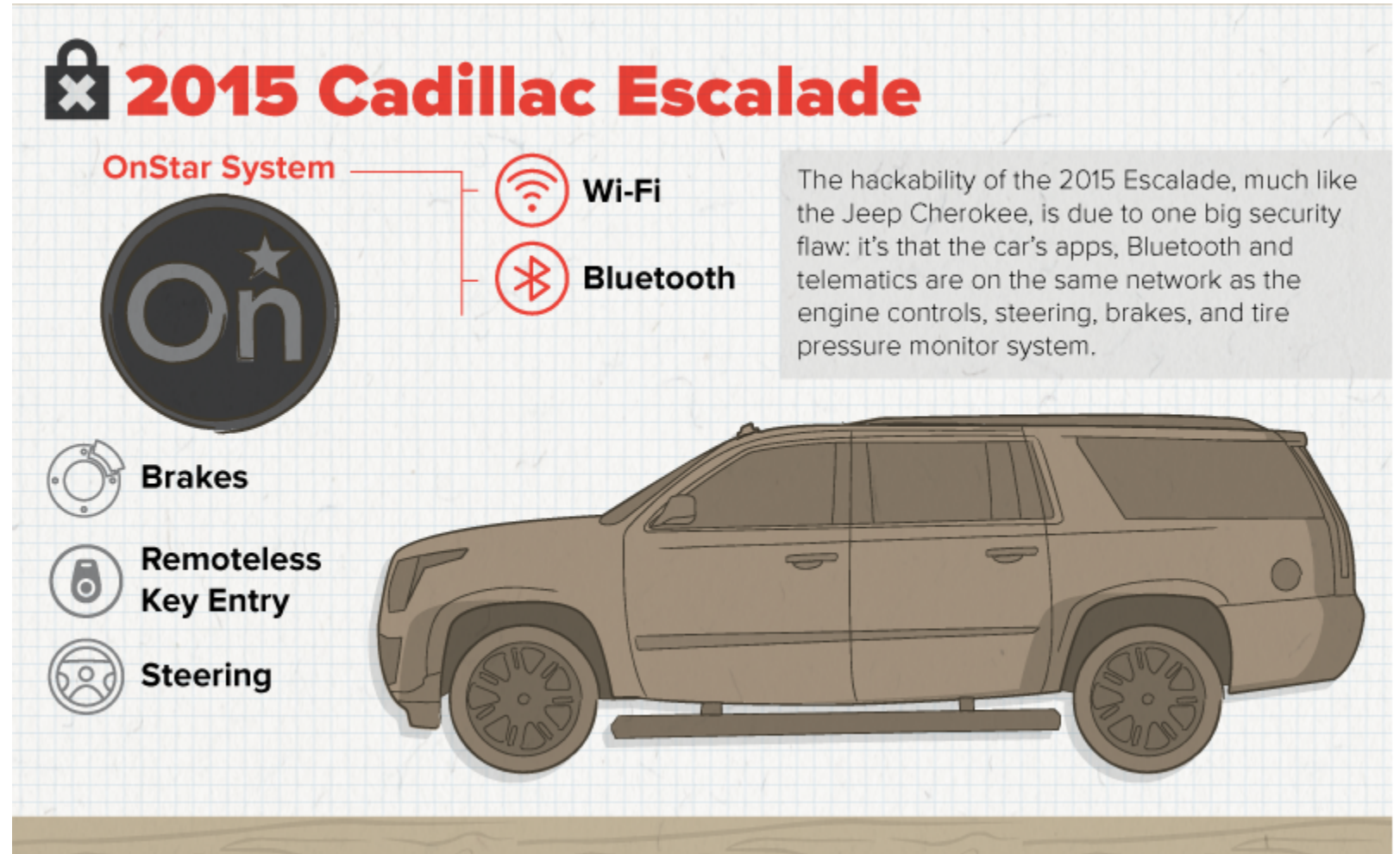


<https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1>

IoT Security Risks

- Hacking

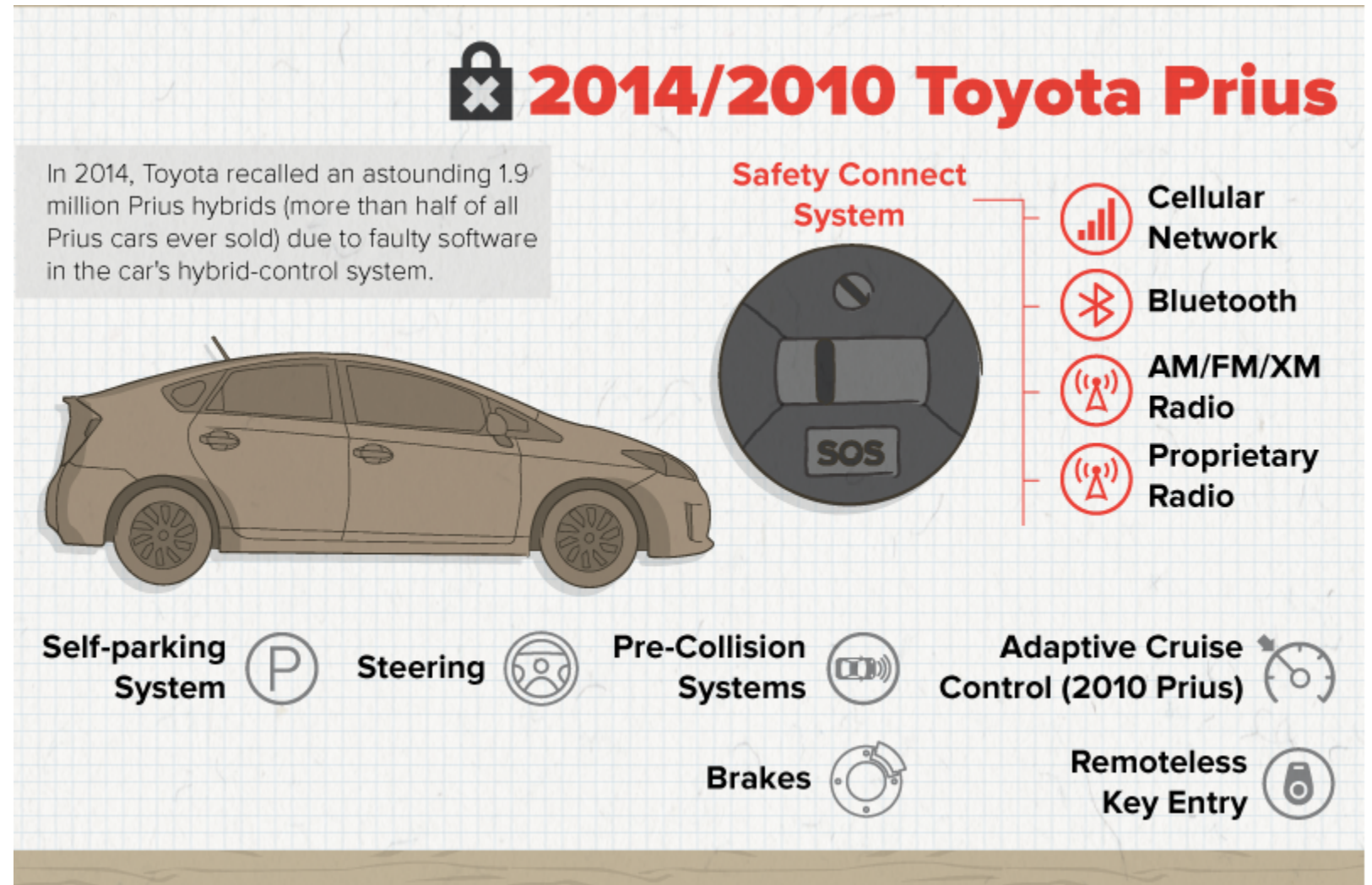
- Connected vehicles



<https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1>

IoT Security Risks

- Hacking
 - Connected vehicles

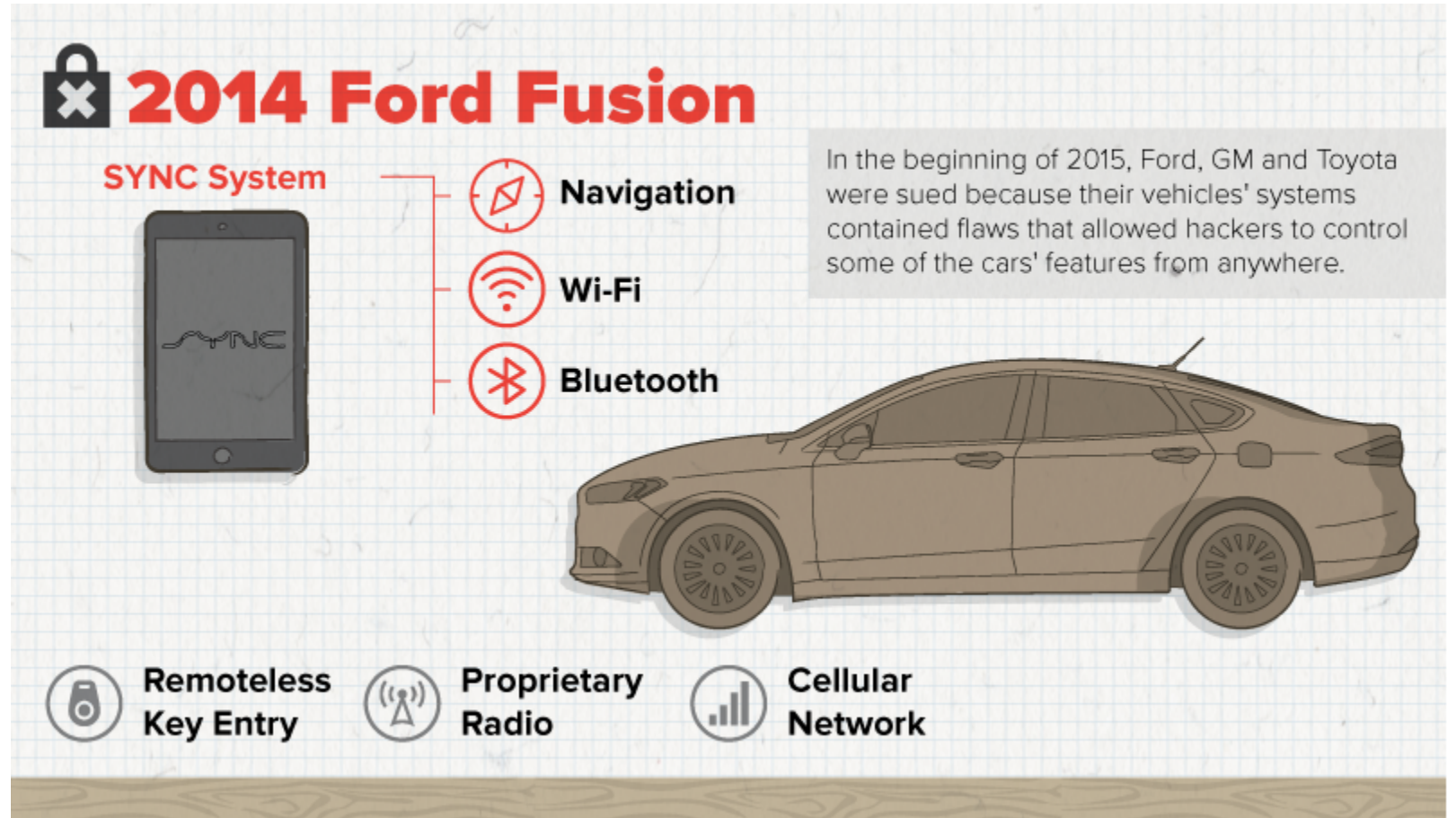


<https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1>

IoT Security Risks

- Hacking

- Connected vehicles



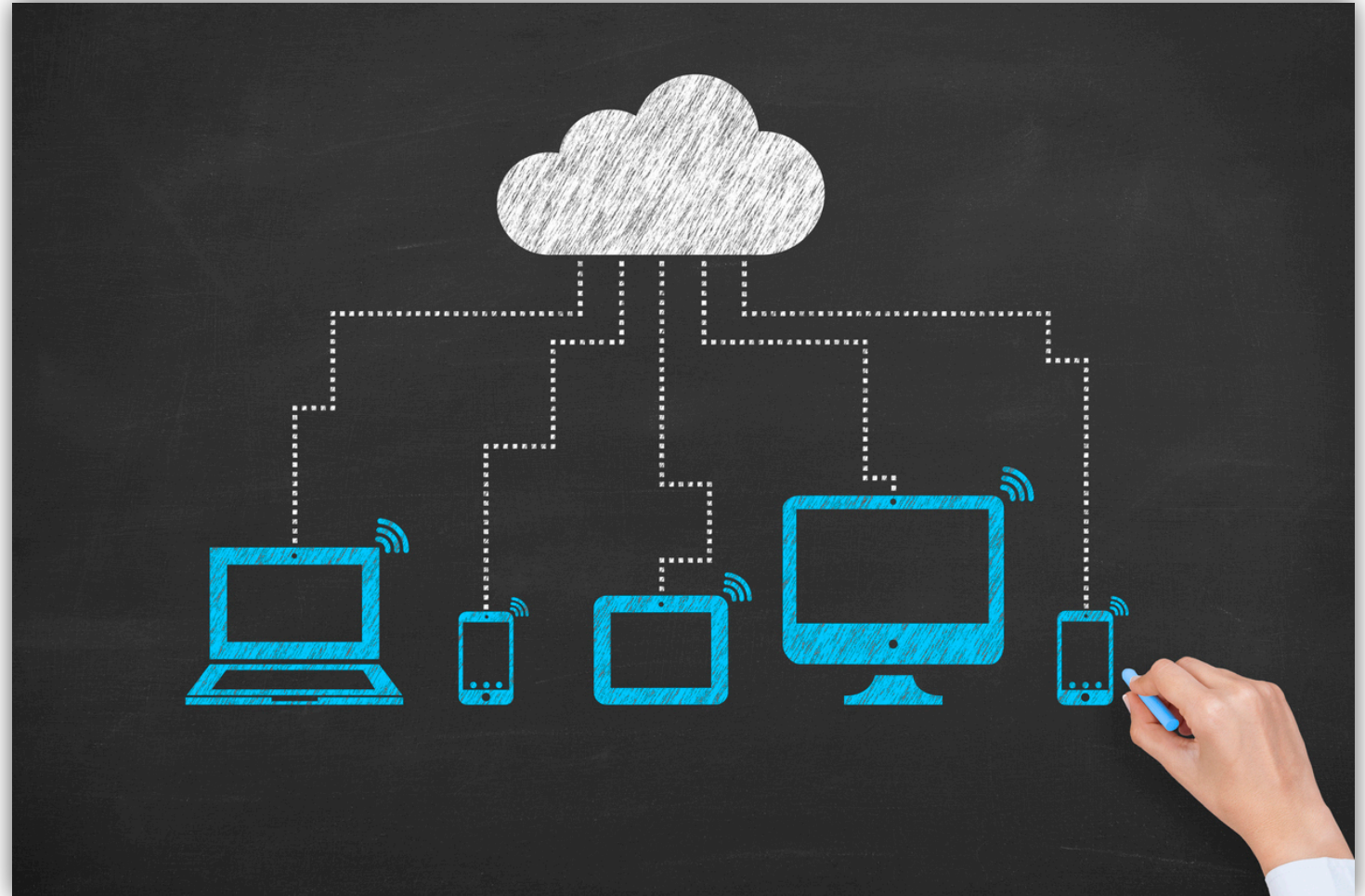
<https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1>



DATA SILOS

Data Silos

- IoT Devices lack
 - Processing power
 - Storage capacity
 - Transmission capabilities
- Data silos are
 - Computers
 - Cell phones
 - Online accounts



WEARABLE DEVICES

IoT Investigations

- Wearable Technology
 - Cell Phone Forensics
 - Data contained in apps themselves
 - Computer Forensics
 - Data contained in online accounts and local computer
 - Wearable Forensics
 - Data contained on actual wearable



IoT Devices

- **Garmin Fenix 5X**

- Unlimited timeline of activity / currently 1.5 years.



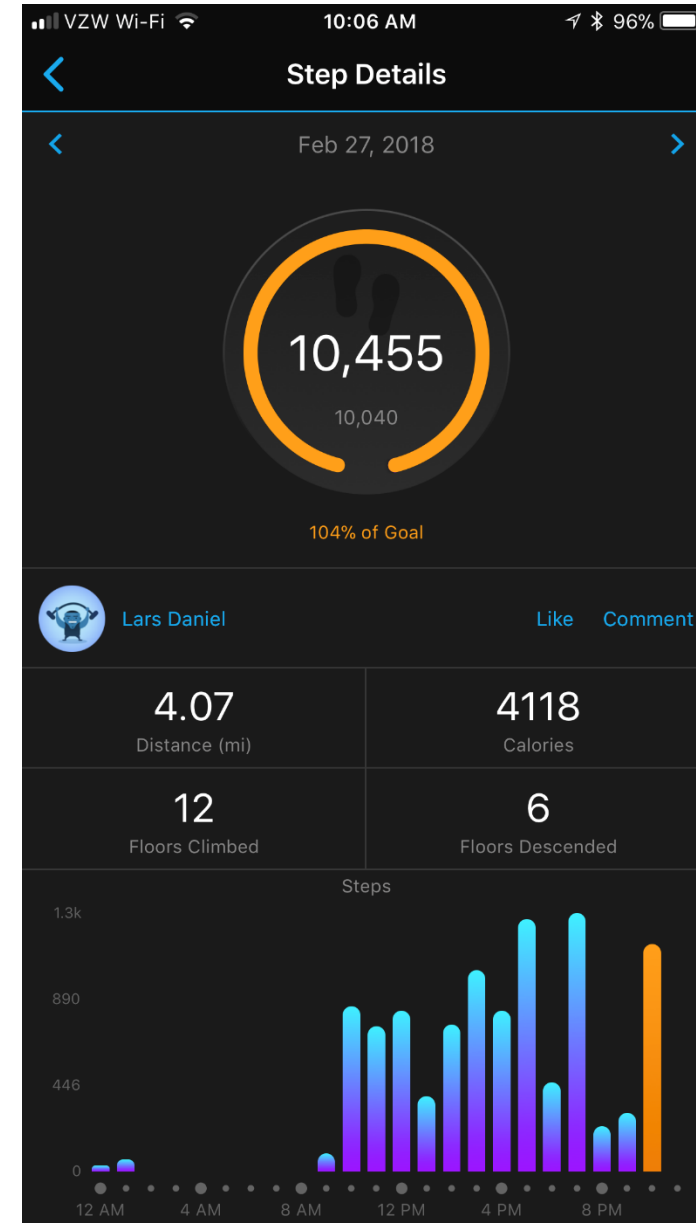
IoT Devices

- **Garmin Fenix 5X**
 - Tracks almost everything about me



IoT Devices

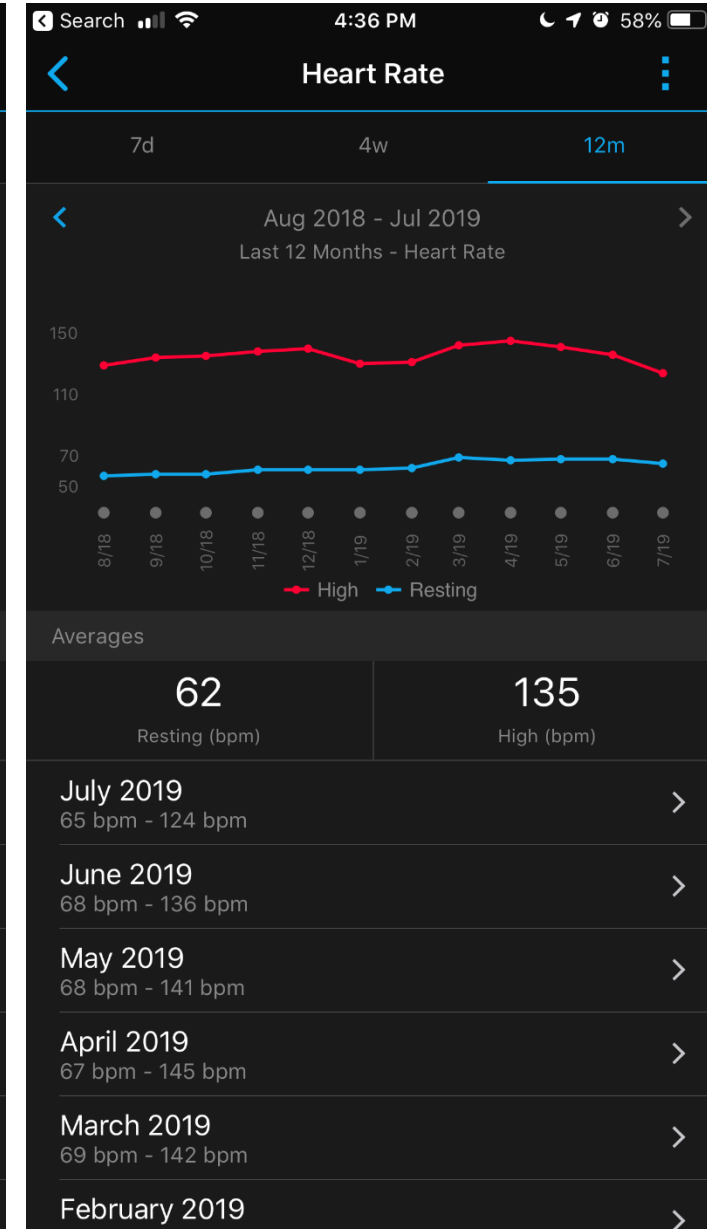
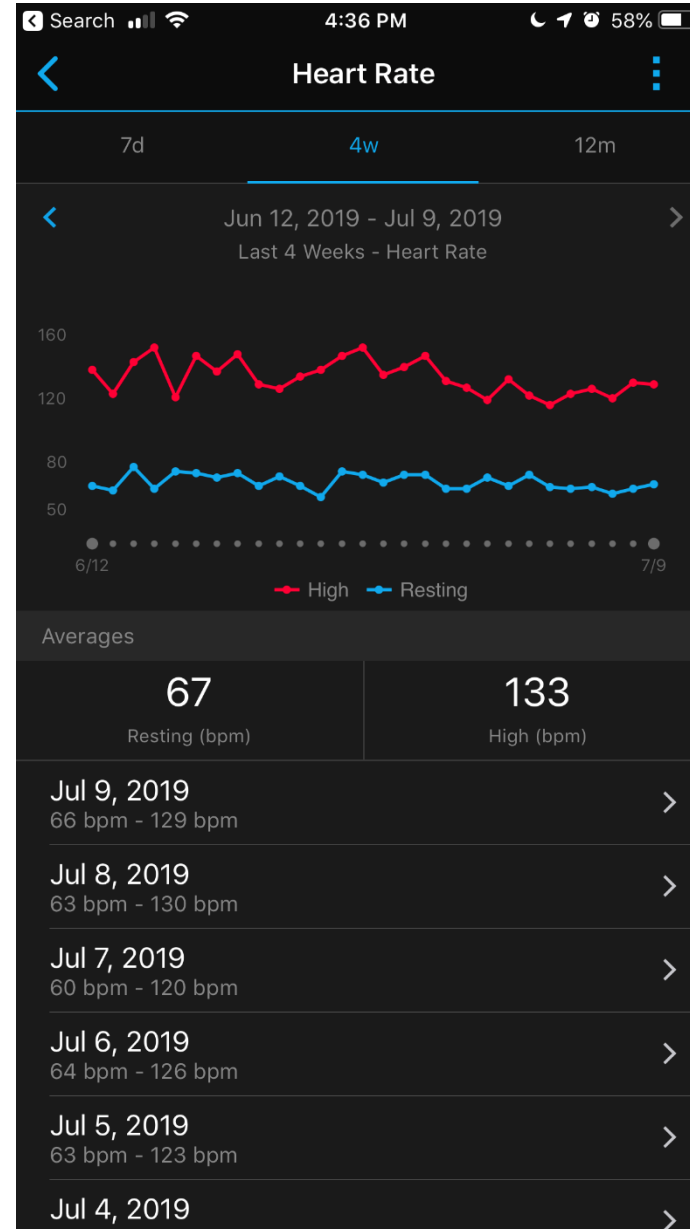
- **Garmin Fenix 5X**
 - Tracks my performance metrics
 - Daily steps and when they were taken



IoT Devices

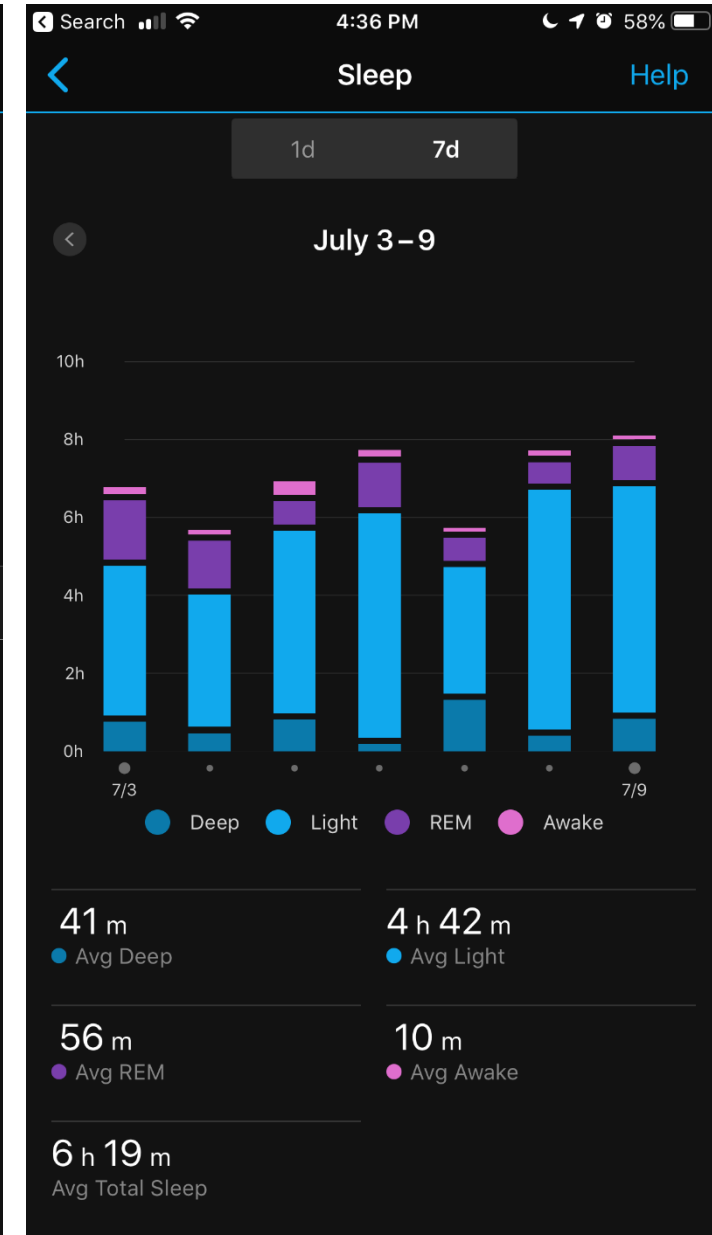
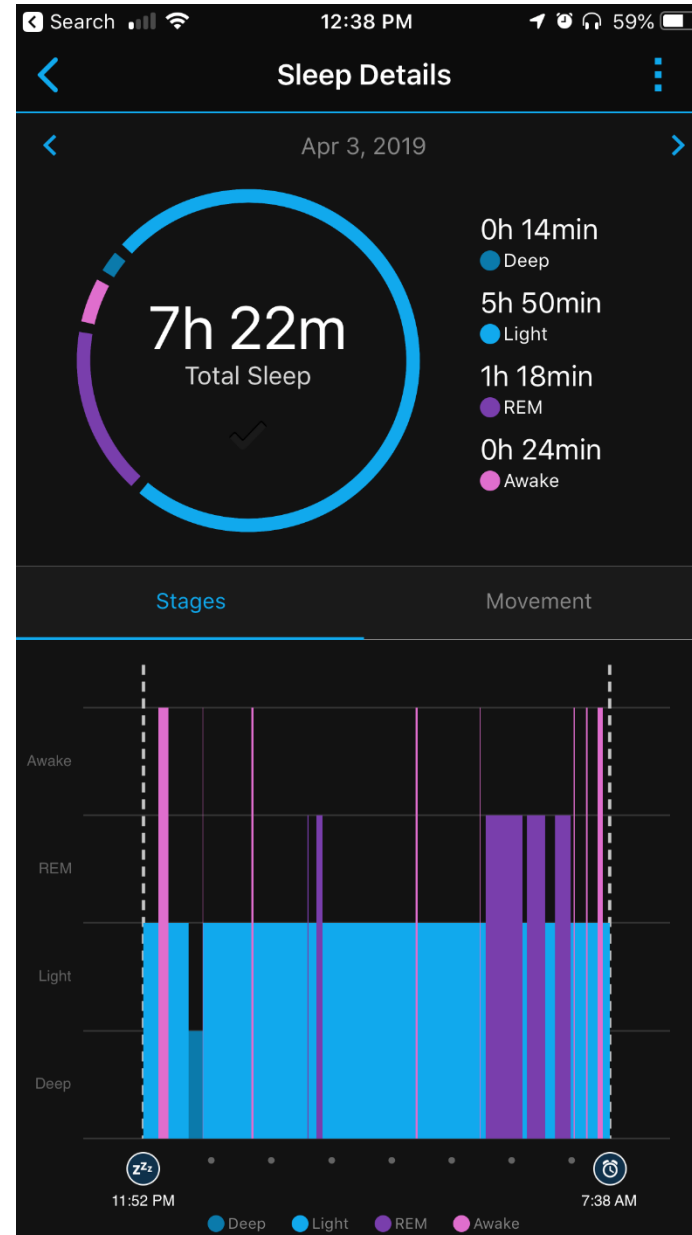
- **Garmin Fenix 5X**

- Tracks almost everything about me
 - Down to the minute heartrate tracking



IoT Devices

- **Garmin Fenix 5X**
 - Tracks sleep down to the minute



IoT Devices

- **Garmin Fenix 5X**
 - Tracks almost everything about me
 - Stress analytics based upon heart rate and HRV (heart rate variability)



IoT Devices

- Garmin Fenix 5X

- Tracks almost everything about me
 - Location activity, routes, maps, saved segments
 - Can contain maps inside the watch for almost the entire world



Fitness Wearables

- Fitness wearable (FitBit)

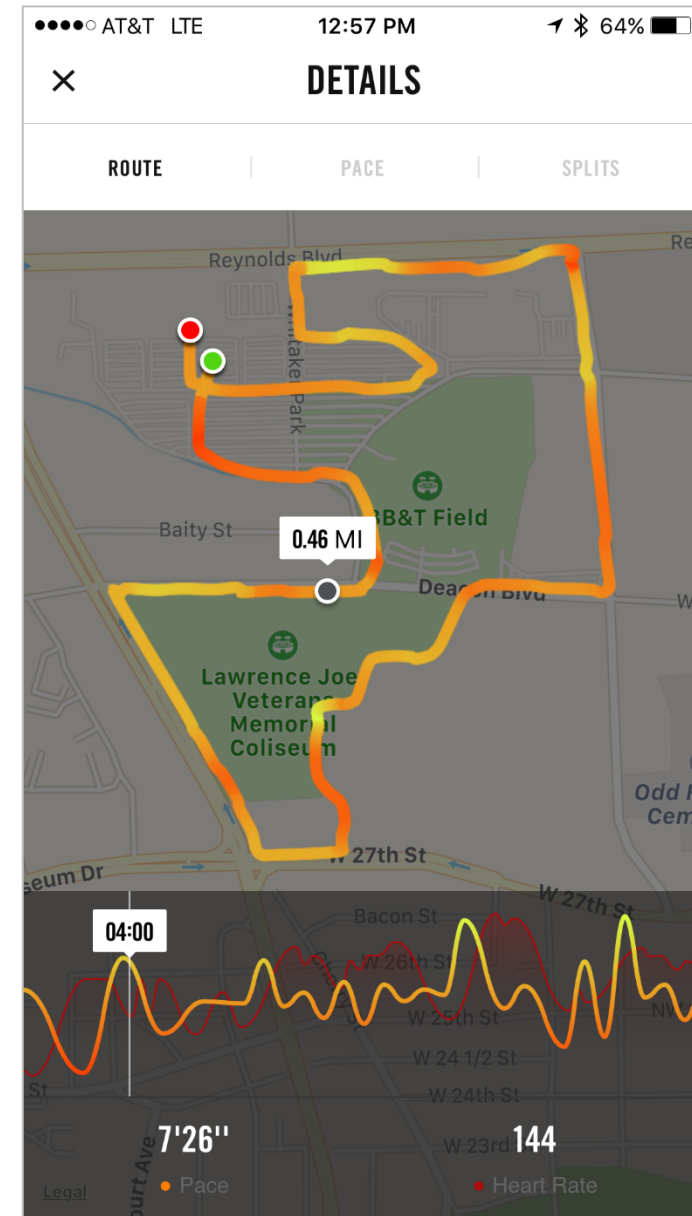
- Victims husband told police that he was at home fighting off an intruder when his wife returned from the gym no later than 9 am. According to the husband, the intruder then shot his wife, tied him up, and ran out of the house. The police searched the wife's fitness wearable. Its data showed that the wife was still moving about the home a distance of 1,217 feet between 9:18 am and 10:05 am...he was having an affair and attempting to cash in on wife's life insurance



<https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>.

Border Crossing

- Did defendant cross the border?
 - Data acquired from online account and the cell phone



Running at time of incident?

- Was suspect using treadmill?
 - Workout can be created after the fact – will be missing some data.



Did cyclist slow down?

- IoT Devices

- Data Silo = Phone Application



Vector™ 3/3S

Measure power at the pedal to gauge your performance.



fēnix® 5 Series

Premium multisport GPS watches available in three sizes and a variety of styles, all featuring wrist-based heart rate



MEDICAL DEVICES

INGESTIBLES AND INSERTABLES

Medical Ingestibles

- Late 2017

- US Food and Drug Administration (FDA) approved first digital pill for general human consumption.
 - Part medication delivery system, part IoT device.
 - Inserted within tablet is an ingestible sensor
 - Tracks exact moment pill hits the stomach



Medical Ingestibles

- Proteus Digital Health

- Designed to address patient non-compliance
 - 20 to 30 percent of patient prescriptions are never filled.
 - 50 percent of medications for chronic diseases are not taken as prescribed.
 - Typically, only one-half of a full prescription is consumed by the patient.
 - Non-compliance causes approximately 125,000 deaths annually and 10 percent of all hospitalizations.
 - This costs U.S. hospitals somewhere between \$100 and \$289 billion annually.

Medical Ingestibles

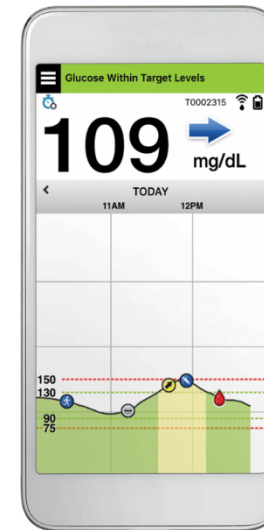
- Proteus Digital Health
 - Proteus Discover

Proteus Discover consists of an ingestible sensor the size of a grain of sand, a small wearable sensor patch, an application on a mobile device and a provider portal. The patient activates Proteus Discover by taking medication with an ingestible sensor. Once the ingestible sensor reaches the stomach, it transmits a signal to the patch worn on the torso. A digital record is sent to the patient's mobile device and then to the Proteus cloud where with the patient's permission, healthcare providers and caregivers can access it via their portal. The patch also measures and shares patient activity and rest.



Medical Implants

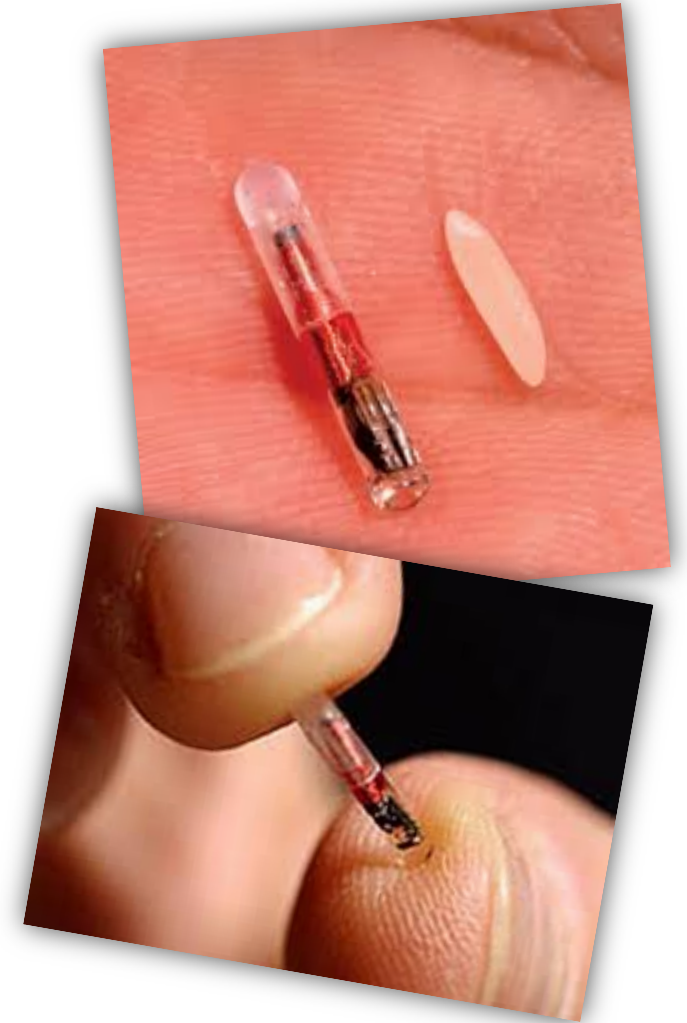
- Eversense CGM (Continuous Glucose Monitoring)
 - Remote monitoring by friends/family and providers via mobile app



Medical Implants

- Verichip

- The US Food and Drug Administration has approved Verichip, an implantable radiofrequency identification device for patients, which would enable doctors to access their medical records. Doctors hope that use of the device will result in be better treatment for patients in emergencies or when a patient is unconscious or lacks medical records. Some people have raised fears, however, that it could lead to infringements of patients' privacy. The chip is the size of a grain of rice and is implanted under local anaesthesia beneath the patient's skin in the triceps area of the right arm, where it is invisible to the naked eye. It contains a unique 16 digit identification number. A handheld scanner passed near the injection site activates the chip and displays the number on the scanner. Doctors and other medical staff use the identification number to access the patient's records on a secure database via encrypted internet access.





SMART VEHICLES

IoT Investigations

- Vehicle Forensics

- In-vehicle infotainment
- Vehicle telematics

- Data types

- 3rd party application data
- USB, Bluetooth, WiFi connections
- Call logs, contact lists, messages
- Pictures, videos, social media feeds
- Location data, navigation information
- Event data with associated time and location



IoT Investigations

- Vehicle Forensics
 - In-vehicle infotainment
 - Vehicle telematics
- Connected devices

iVe - Infotainment & Vehicle System Forensics

File View Maps Report Export Tools

CONTENT

- Applications
- Connections
 - Bluetooth (36)
 - Wifi (3)
- Devices (104)**
 - Erin's iPhone
 - Ben's iPhone
 - Will Jace Herondale
 - KINGSTON
 - T7380
 - rolo
 - blemere's iPod
 - dd-wpa2-aes-ch8
 - dd-wpa2-tkip-ch10
 - dd-wep-ch1
 - Jennifer's iPhone
 - motorola XT907
 - Charee's iPhone
 - SAMSUNG Electronics Co. Ltd. SCH-I605
 - Tiffany's iPhone
 - USB Hard Disk Drive DSK5:
 - M.O Ironti (SM-N900T)
 - Adrian Helmick's iPhone
 - iPhone
 - Sara Lee's iPhone
 - 64A3CB30CE8E
 - 380F4A5AD378
 - 38E7D8937381
 - 406AAB953E4D
 - 50A4C85F4847

SYSTEMS

CONTENT

TAGS

SEARCH

Grid

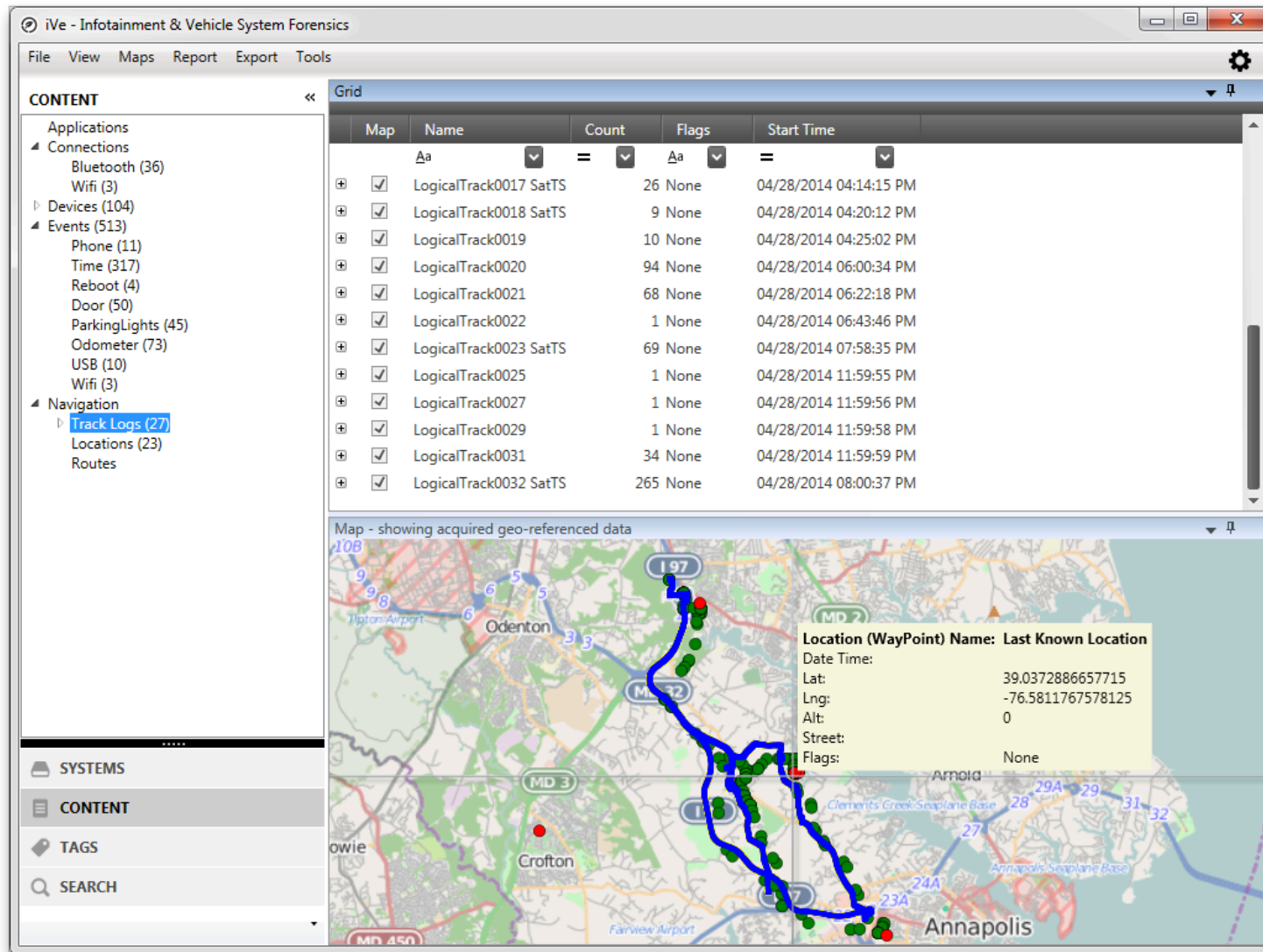
Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Ty
Erin's iPhone	2	Phone-2	A888083AE07F	Bluetooth Address
Erin's iPhone	5	Phone-5	0	Bluetooth Address
Erin's iPhone			DQGV412FH1G	Serial Number
iPhone	3	Phone-3	FFFFFFFFE0864D97	Bluetooth Address
iPhone	5	Phone-5	0	Bluetooth Address
iPhone			F2LLP20EFNJP	Serial Number
Jennifer's iPhone	2	Phone-2	0	Bluetooth Address
Jennifer's iPhone	5	Phone-5	0	Bluetooth Address
Jennifer's iPhone	3	Phone-3	FFFFFFFFCB30CE8E	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
Lexisss iPhone			DNQJPXBVF8GH	Serial Number
M.O Ironti (SM-N900T)	3	Phone-3	11AB0E57	Bluetooth Address
motorola XT907	4	4	0	Bluetooth Address
motorola XT907			99000201667977	Serial Number
rolo	3	Phone-3	E899C43E8A97	Bluetooth Address
rolo	2	Phone-2	E899C43E8A97	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605	4	4	0	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605			43007cae2eff3011	Serial Number
Sara Lee's iPhone	3	Phone-3	FFFFFFFFB77F40AC	Bluetooth Address
T7380	3	Phone-3	38E7D825E758	Bluetooth Address
Tiffany's iPhone	5	Phone-5	0	Bluetooth Address
USB Hard Disk Drive DSK5:	1	USB-1	0	Bluetooth Address
USB Hard Disk Drive DSK5:			-950332193	Serial Number
Will Jace Herondale	5	Phone-5	0	Bluetooth Address
Will Jace Herondale			7003588MA4S	Serial Number

Map

Display of records selected

IoT Investigations

- Vehicle Forensics
 - In-vehicle infotainment
 - Vehicle telematics
- Track logs



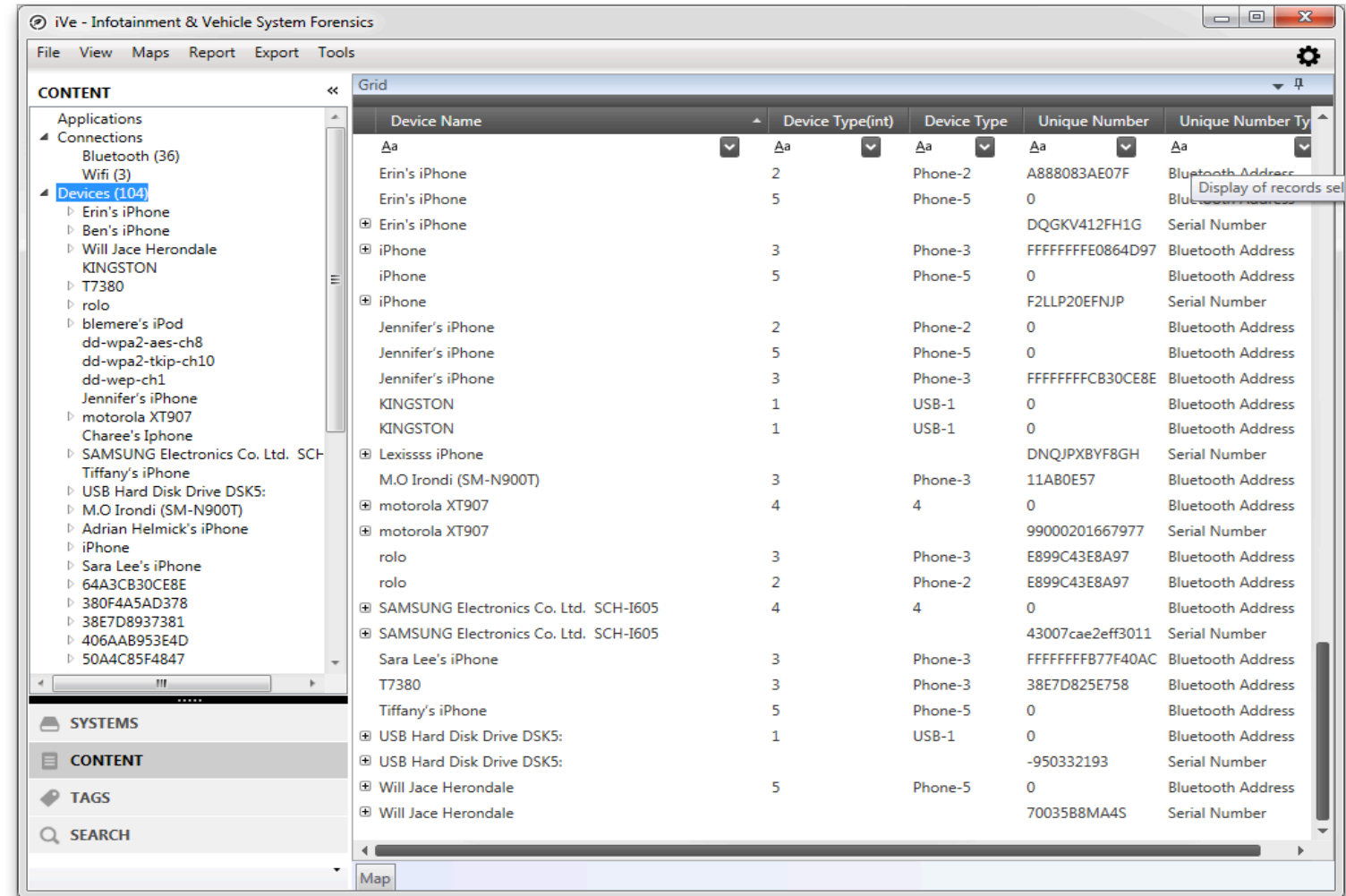
IoT Investigations

- Vehicle Forensics

- In-vehicle infotainment
- Vehicle telematics

- Velocity Logs

- Vehicle velocity and corresponding timestamp



iVe - Infotainment & Vehicle System Forensics

File View Maps Report Export Tools

Grid

Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Ty
Erin's iPhone	2	Phone-2	A888083AE07F	Bluetooth Address
Erin's iPhone	5	Phone-5	0	Bluetooth Address
Erin's iPhone			DQGKV412FH1G	Serial Number
iPhone	3	Phone-3	FFFFFFFFE0864D97	Bluetooth Address
iPhone	5	Phone-5	0	Bluetooth Address
iPhone			F2LLP20EFNJJP	Serial Number
Jennifer's iPhone	2	Phone-2	0	Bluetooth Address
Jennifer's iPhone	5	Phone-5	0	Bluetooth Address
Jennifer's iPhone	3	Phone-3	FFFFFFFFC830CE8E	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
Lexissss iPhone			DNQJPXBYF8GH	Serial Number
M.O Irondi (SM-N900T)	3	Phone-3	11A80E57	Bluetooth Address
motorola XT907	4	4	0	Bluetooth Address
motorola XT907			99000201667977	Serial Number
rolo	3	Phone-3	E899C43E8A97	Bluetooth Address
rolo	2	Phone-2	E899C43E8A97	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605	4	4	0	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605			43007cae2eff3011	Serial Number
Sara Lee's iPhone	3	Phone-3	FFFFFFFFF877F40AC	Bluetooth Address
T7380	3	Phone-3	38E7D825E758	Bluetooth Address
Tiffany's iPhone	5	Phone-5	0	Bluetooth Address
USB Hard Disk Drive DSK5:	1	USB-1	0	Bluetooth Address
USB Hard Disk Drive DSK5:			-950332193	Serial Number
Will Jace Herondale	5	Phone-5	0	Bluetooth Address
Will Jace Herondale			7003588MA4S	Serial Number

Map

Teleporting Car?

- Rental car location records
- Original data needed.





SMART HOME

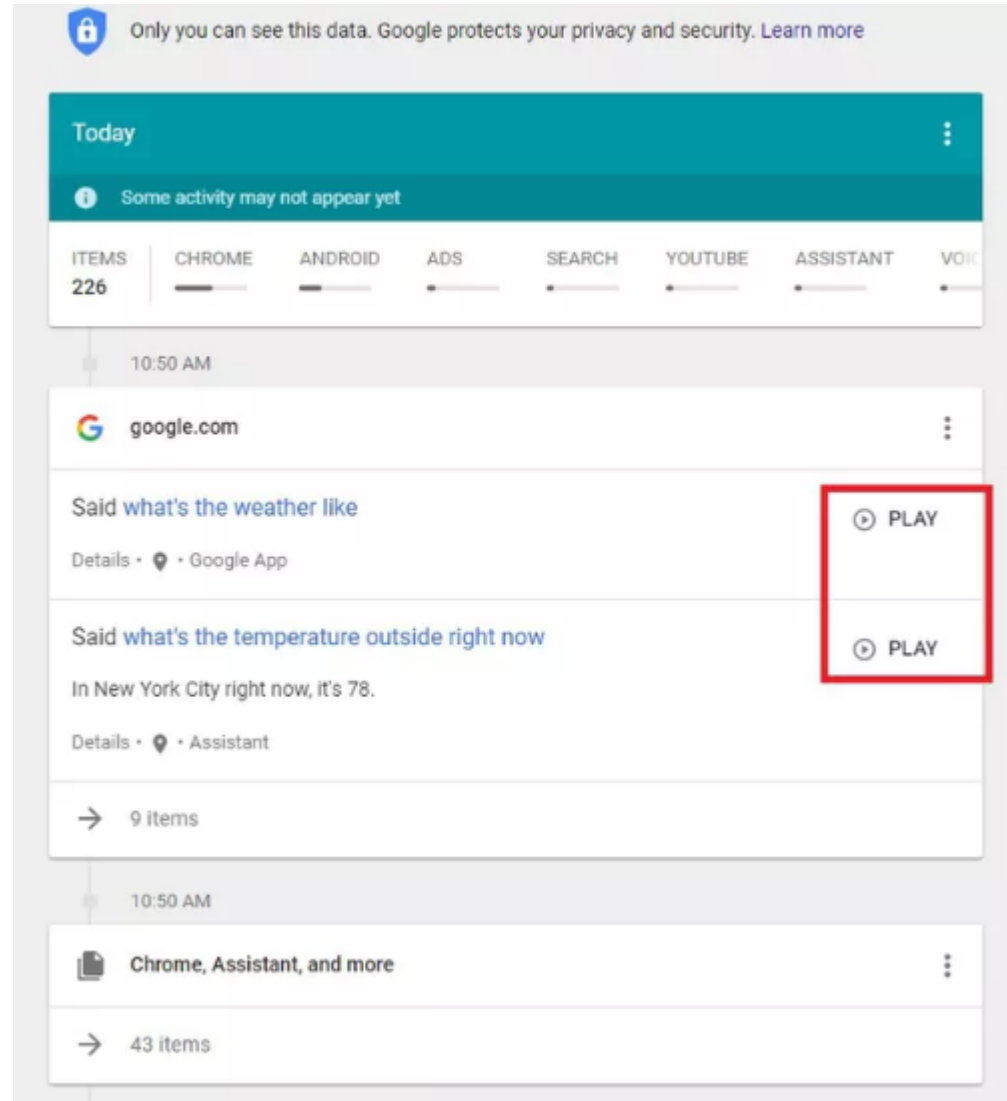
Alexa as a home assistant

- Murder case - *Arkansas v. Bates*, No. CR-2016-370 (Cir. Ct. Benton County, Arkansas).
 - Police seized the defendant's smart speaker believing it might contain evidence of what happened the night of the murder at defendant's home.
 - Amazon moved to quash warrant, contenting 1st amendment rights to publish and speak through the speaker
 - Motion later mooted when defendant gave manufacturer permission to turn over audio recordings
 - Recordings kept by Amazon, organized and identifiable (not-anonymized for "research")
 - Only contained provider side

<https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>

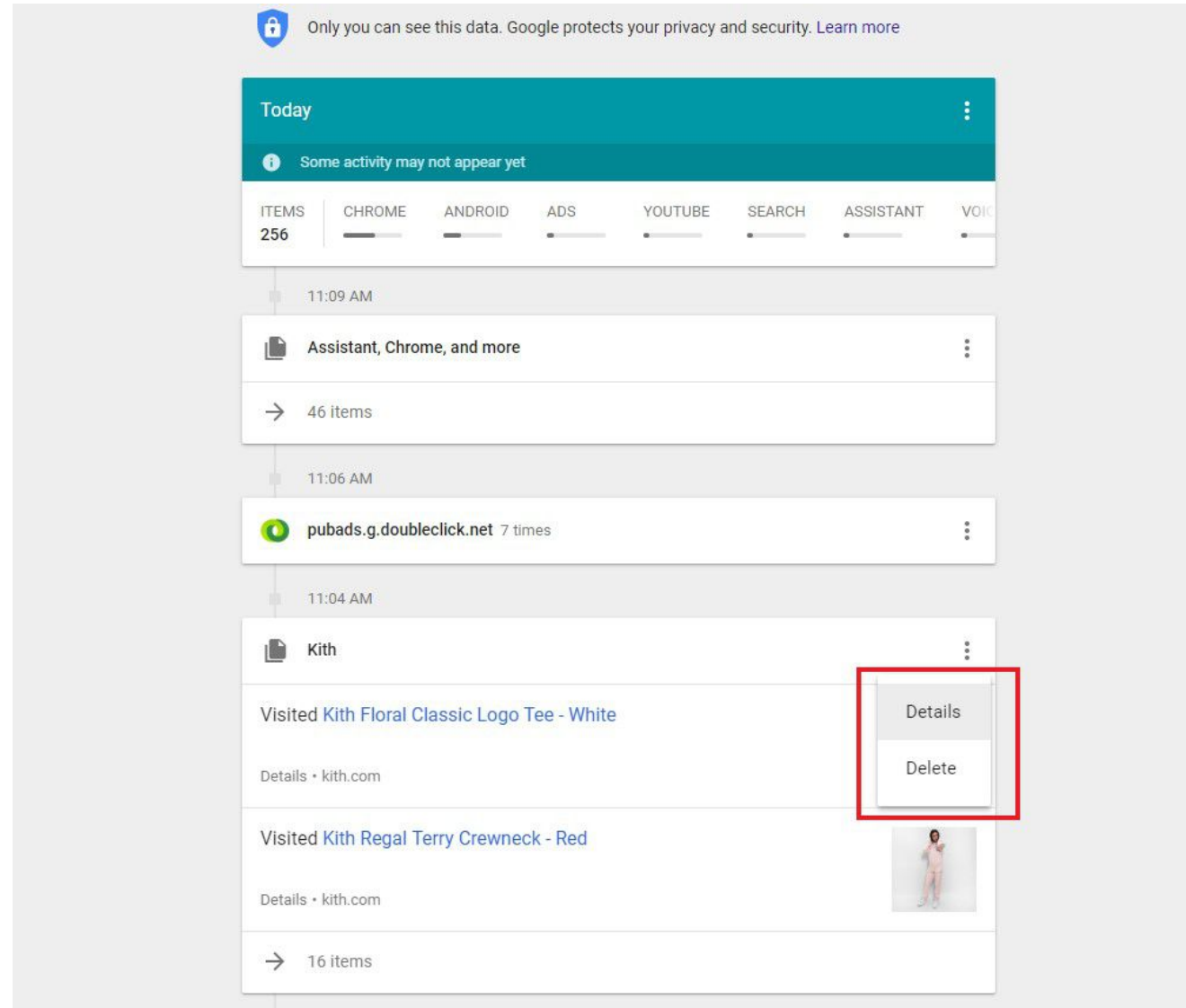
Smart Home Assistants

- Google Home
 - Google queries



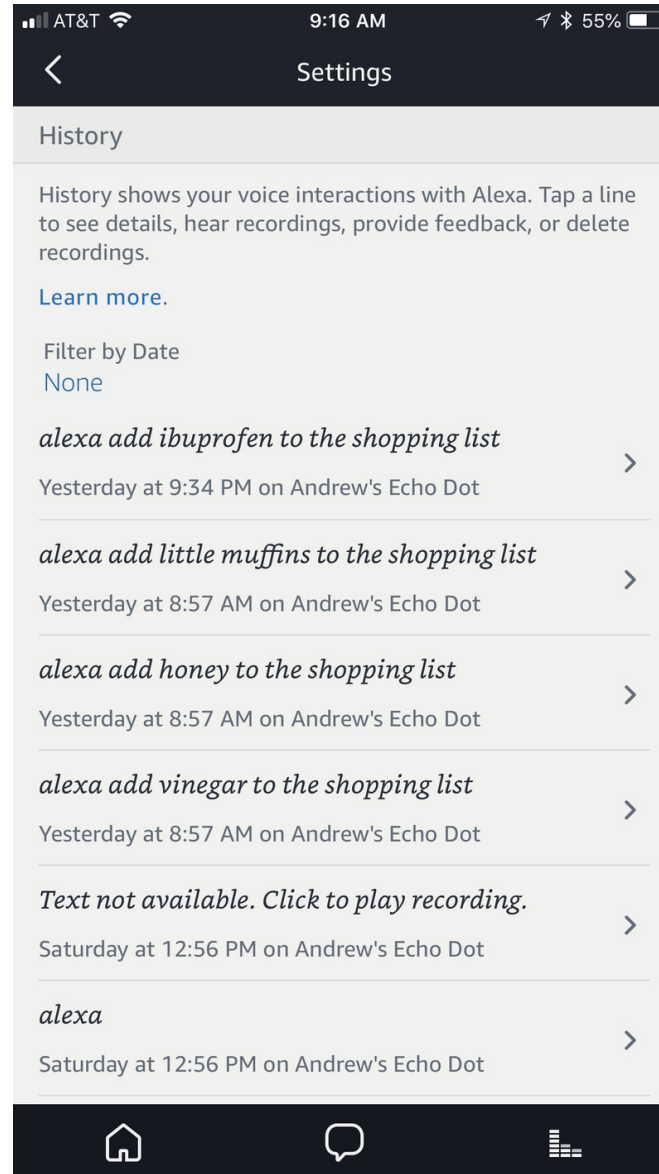
Smart Home Assistants

- Google Home
 - Shopping



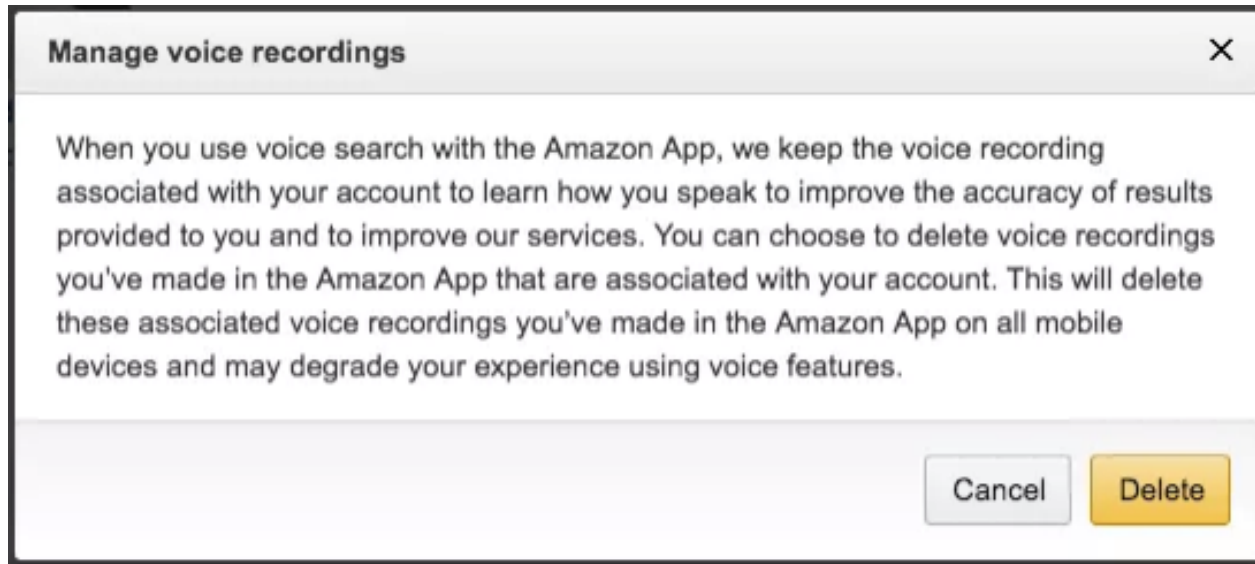
Smart Home Assistants

- Amazon Alexa
 - Search queries



Smart Home Assistants

- Amazon Alexa
 - Voice recordings



Smart Home Assistants

- Interrogate the device
 - Low tech works too...
 - Careful with the Christmas lists!



Smart Home Security

- Recording video
- Timeline data
- Account data



Smart Home Security

- Recording video
- Timeline data
- Account data
- Hidden microphone

Business

Google failed to notify customers it put microphones in Nest security systems



https://www.washingtonpost.com/business/2019/02/20/google-forgot-notify-customers-it-put-microphones-nest-security-systems/?noredirect=on&utm_term=.cfa73cc39212

Smart Home Security

- Nest – Neighbors home



Smart Home Security

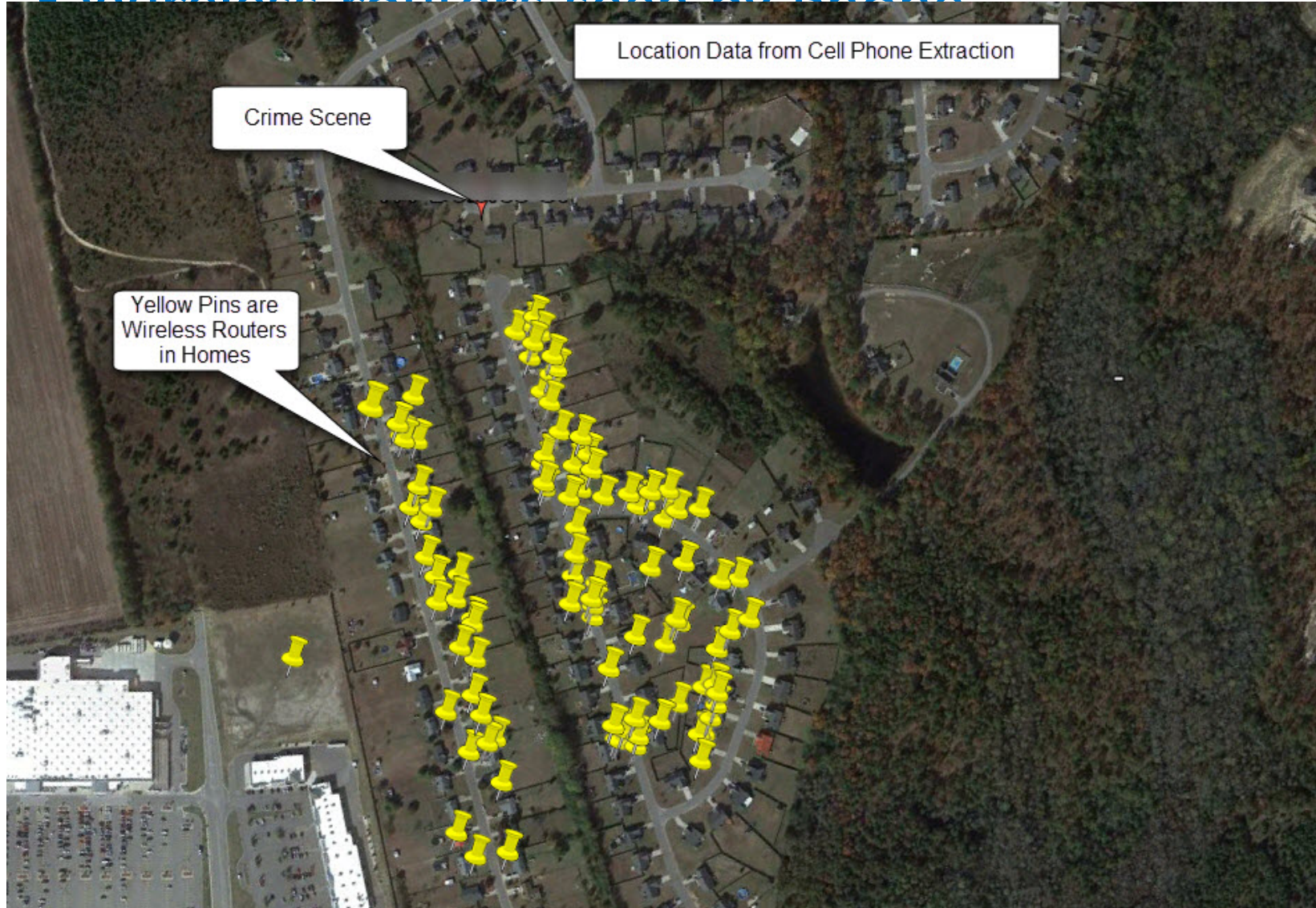
- Nest – Neighbors home



CASE EXAMPLES

Case Example: WiFi Phone Location

• Wireless routers seen by phone



- Wireless Networks

Wireless Network		Go to ▾
BSSID:	e4:f4:c6:0b:5f:51	
SSID:	Bill Wi the Science Fi	
Security Mode:		
Last Connected:		
Last Auto Connected:		
Timestamp:	4/1/2016 9:30:32 AM(UTC-4)	
End Time:		
Package:	GooglePlay	
Extraction:	File System	
Source file:		
Map		
Position:	15° 40' 00" N 78° 00' 00" W	
Map Address:	15° 40' 00" N 78° 00' 00" W	

Examination of Plaintiff's Phone

- Application data
 - Synced to account
 - and phone

Time	Category	Item
11:48:44 AM(UTC-6)	DB	Phone (dialer.db)
11:48:44 AM(UTC-6)	Text File	com.android.dialer.xml
11:48:47 AM(UTC-6)	Picture	1841 task_thumbnail.DELETED.png
11:48:55 PM(UTC-6)	E-Mail	Received E-Mail from [REDACTED] (Assistant Services)
11:49:17 AM(UTC-6)	SMS From: [REDACTED] Mother	Ohhhh, well if it can be gotten for less than \$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trins would nmhahlv break even with \$12 delivered
11:49:17 AM(UTC-6)	SMS From: [REDACTED] Mother	Ohhhh, well if it can be gotten for less than \$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trins would nmhahlv break even with \$12 delivered
11:51:02 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED.xml
11:52:23 PM(UTC-6)	Text File	event data [REDACTED]
11:55:47 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 1.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.auth.devicesignals.DeviceSignalsStore.DELETED.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.tapandpay.service.TapAndPayServiceStorage.DELETED.xml
11:55:48 AM(UTC-6)	Text File	settings_secure.DELETED.xml
11:56:14 AM(UTC-6)	Picture	1843 task_thumbnail.png
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	DB	Gmail (Cookies)
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.xml
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.DELETED.xml
11:59:39 AM(UTC-6)	Text File	Account [REDACTED].DELETED.xml
11:59:58 AM(UTC-6)	Text File	com.google.android.gms.auth.authzen.cryptauth.DeviceStateSyncManager.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD BREATHS.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD NOTIF.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.TOUCH.DELETED.xml
12:00:05 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED 1.xml
12:00:05 AM(UTC-6)	Text File	DebugAnalytics.DELETED 1.xml
12:00:20 PM(UTC-6)	Picture	IMG [REDACTED] 120016201.jpg
12:00:23 PM(UTC-6)	DB	Google Photos (media store extras)
12:00:23 PM(UTC-6)	Picture	IMG [REDACTED] 120021204.jpg
12:00:23 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 4.xml
12:00:24 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 2.xml
12:00:24 PM(UTC-6)	Picture	IMG [REDACTED] 120022835.jpg
12:00:24 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 3.xml
12:00:25 PM(UTC-6)	DB	Google+ (trash.db)
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 2.xml
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 5.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 1.xml
12:00:58 PM(UTC-6)	Text File	MailAppProvider.DELETED 1.xml
12:00:59 AM(UTC-6)	Text File	Pmaps.xml
12:00:59 PM(UTC-6)	Text File	Account [REDACTED].DELETED 1.xml
12:00:59 PM(UTC-6)	Text File	MailAppProvider.DELETED.xml

Case Study: Distracted Driving

- Detailed timeline analysis at point of impact
 - Cell phone, event data recorder, online accounts



Case Example: Cell Phone Picture

- Photo Editing and Metadata
 - Web based (cloud) photo editing application



Metadata Facts			
Serving size	Serving per Container		
Amount per serving	Calories		
Logical Size		% Daily Value*	
Physical Size	...g		...%
Modified Date	...g		...%
Accessed Date	...g		...%
Created Date	...g		...%
File Type	...g		...%
File Name	...g		...%
Version	...g		...%
Location (Path)	...g		...%
Page Count	...%	Line Count	...%
Paragraph Count	...%	Word Count	...%
*Percent Daily Values are based on 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.			



Civil Case Becomes Criminal

- Data theft turns criminal
 - Assisting Federal Marshalls
 - Data thief becomes a fugitive
 - Syncing between IOT devices preserved deleted data

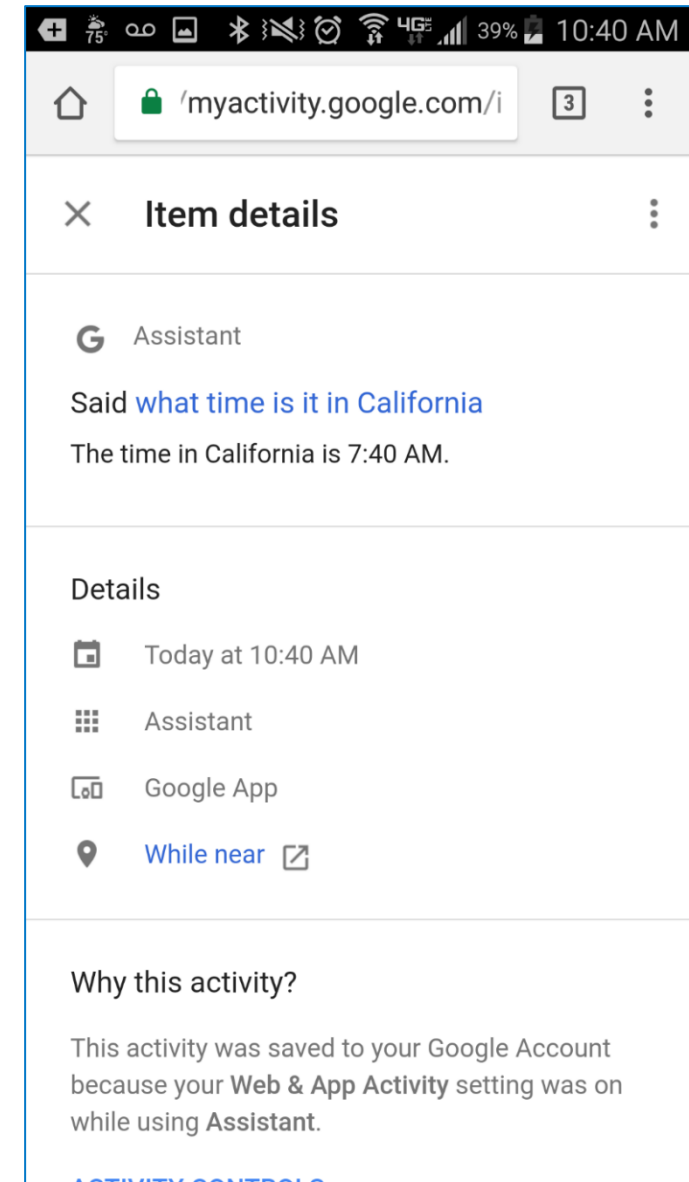
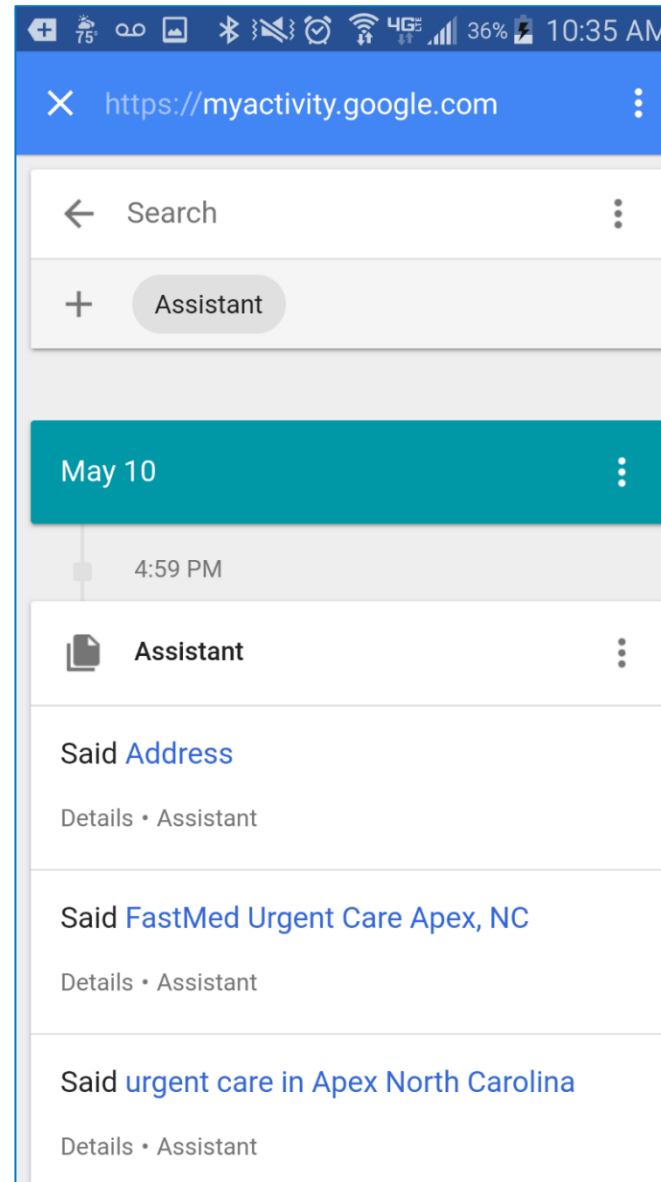


11. There is also a photograph stored on the Cell Phone that appears to be a picture of a New Mexico driver's license in the name of [REDACTED] with the date of birth of XX/XX/19XX. A copy of the photograph with the date of birth redacted is attached hereto as Exhibit 4.

<u>Cell Phone:</u>	Hey! Want to make some fast cash?
[REDACTED] <u>Number:</u>	Who is this
<u>Cell Phone:</u>	[REDACTED] You moved my lazy boy chairs about 2 months ago. I am putting in for a name change and one of the many things they want is an affidavit attesting to my morel [sic] character. They want 2 of them. I already have them both ready to go so now I am just looking for 2 people that will sign them in front of a notary. I am offering \$100 cash per person. Know anyone that might be interested?
[REDACTED] <u>Number:</u>	I will let y
<u>Cell Phone:</u>	Awesome!
[REDACTED] <u>Number:</u>	When and where. When do you have to have this done
<u>Cell Phone:</u>	Whenever is good for you will be fine. We can do it at the UPS store on [REDACTED] I think they have a notary there. If not then any bank would do but i am pretty sure that the UPS store has one.

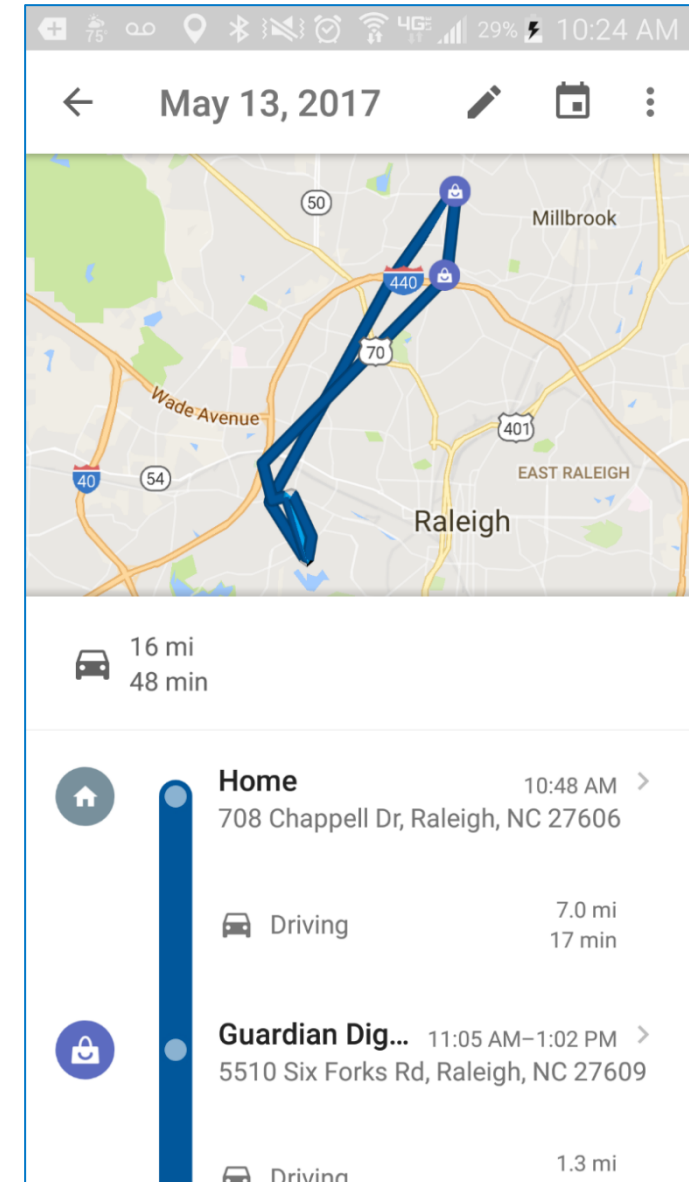
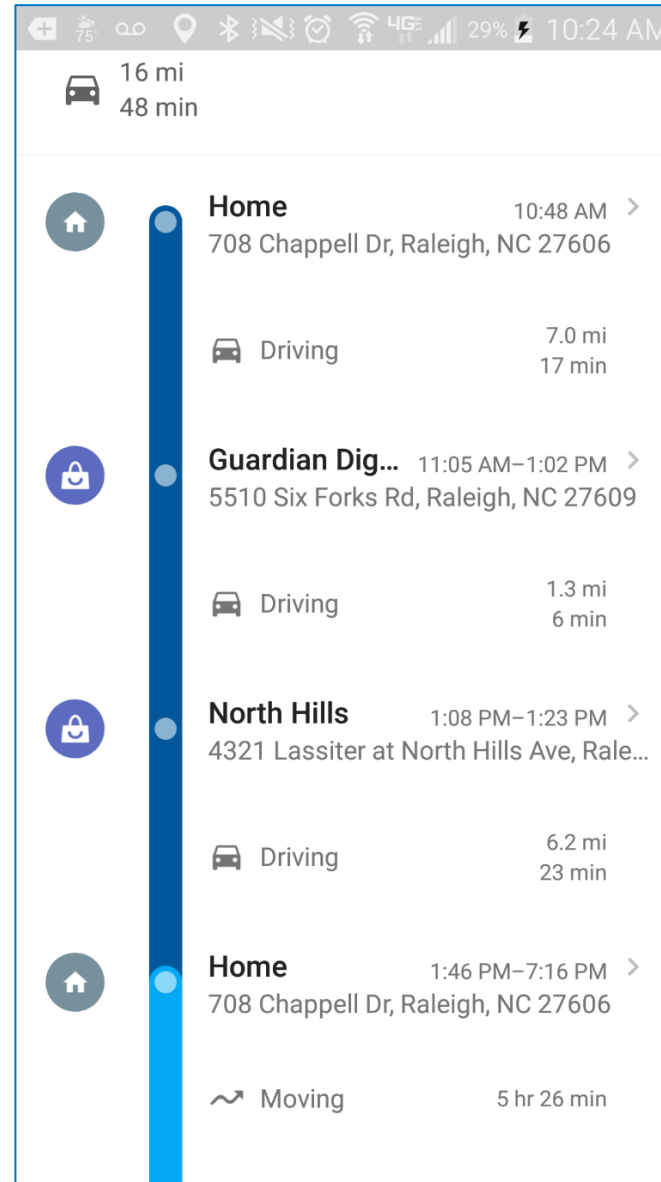
Capabilities: Examples

- Google is listening
 - Location activity
 - Full route



Capabilities: Examples

- Google is listening
 - Location activity
 - Full route



QUESTIONS?

lars.daniel@envistaforensics.com / 919-621-9335

